

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 9 月 5 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 3 1 4 4 6 6
Application Number:

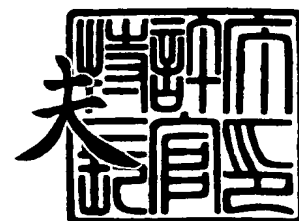
[ST. 10/C] : [J P 2 0 0 3 - 3 1 4 4 6 6]

出 願 人 株 式 会 社 リ コ ー
Applicant(s):

2 0 0 3 年 1 0 月 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 0304083
【提出日】 平成15年 9月 5日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G06F 12/00
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 金井 洋一
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 斉藤 敦久
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 谷内田 益義
【特許出願人】
 【識別番号】 000006747
 【氏名又は名称】 株式会社リコー
【代理人】
 【識別番号】 100070150
 【弁理士】
 【氏名又は名称】 伊東 忠彦
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-269102
 【出願日】 平成14年 9月13日
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-299712
 【出願日】 平成14年10月11日
【手数料の表示】
 【予納台帳番号】 002989
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9911477

【書類名】 特許請求の範囲**【請求項 1】**

暗号化されたドキュメントファイルの復号鍵を取得する手段と、
取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、
上記ドキュメントファイルに関連付けられている印刷要件をネットワークを介してサーバから取得する手段と、
取得した上記印刷要件を満たす印刷処理を実行させる手段とを備えたことを特徴とするドキュメント印刷プログラム。

【請求項 2】

上記サーバに対してユーザの認証を行う手段と、
認証した上記ユーザの印刷要件をドキュメントファイルのセキュリティ属性に関連付けられて組織単位に設けられた A C L から取得する手段とを備えた請求項 1 に記載のドキュメント印刷プログラム。

【請求項 3】

暗号化された上記ドキュメントファイルのセキュリティ属性を上記ドキュメントファイルと関連付けて登録するセキュリティ属性データベースを上記サーバに備えた請求項 2 に記載のドキュメント印刷プログラム。

【請求項 4】

上記セキュリティ属性は文書カテゴリと機密レベルとを含む請求項 3 に記載のドキュメント印刷プログラム。

【請求項 5】

上記サーバに対してユーザの認証を行う手段と、
認証した上記ユーザの印刷要件をドキュメントファイルのセキュリティ属性およびユーザタイプに関連付けられて設けられたセキュリティポリシーから取得する手段とを備えた請求項 1 に記載のドキュメント印刷プログラム。

【請求項 6】

暗号化された上記ドキュメントファイルのセキュリティ属性を上記ドキュメントファイルと関連付けて登録するセキュリティ属性データベースを上記サーバに備えた請求項 5 に記載のドキュメント印刷プログラム。

【請求項 7】

上記セキュリティ属性は文書カテゴリと機密レベルとを含み、上記ユーザタイプはカテゴリとレベルとを含む請求項 6 に記載のドキュメント印刷プログラム。

【請求項 8】

上記ドキュメントファイルを暗号化した暗号鍵に相当するパラメータをネットワークを介してサーバから取得し、このパラメータから復号鍵を導出する請求項 2 または 5 のいずれか一項に記載のドキュメント印刷プログラム。

【請求項 9】

内部で保持もしくは生成したパラメータを上記復号鍵の生成に利用する請求項 8 に記載のドキュメント印刷プログラム。

【請求項 1 0】

上記ドキュメントファイルに含まれるパラメータを上記復号鍵の生成に利用する請求項 8 または 9 のいずれか一項に記載のドキュメント印刷プログラム。

【請求項 1 1】

ドキュメントファイルを暗号化する暗号鍵を取得する手段と、
上記ドキュメントファイルの印刷要件を指定する情報を上記ドキュメントファイルに関連付けてネットワークを介してサーバに登録する手段と、
上記ドキュメントファイルを上記暗号鍵で暗号化する手段とを備えたことを特徴とするドキュメント保護プログラム。

【請求項 1 2】

上記印刷要件を指定するセキュリティ属性を上記ドキュメントファイルと関連付けてサ

サーバに登録する請求項 11 に記載のドキュメント保護プログラム。

【請求項 13】

上記セキュリティ属性を上記ドキュメントファイルと関連付けて登録するセキュリティ属性データベースを上記サーバに備えた請求項 12 に記載のドキュメント保護プログラム。

【請求項 14】

上記セキュリティ属性は文書カテゴリと機密レベルとを含む請求項 13 に記載のドキュメント保護プログラム。

【請求項 15】

暗号化に用いた暗号鍵を上記サーバに登録する請求項 11 に記載のドキュメント保護プログラム。

【請求項 16】

暗号化に用いた暗号鍵の導出に用いたパラメータを上記サーバに登録する請求項 15 に記載のドキュメント保護プログラム。

【請求項 17】

暗号化に用いた暗号鍵の導出に用いたパラメータを上記ドキュメントファイルの一部に付与する請求項 15 または 16 のいずれか一項に記載のドキュメント保護プログラム。

【請求項 18】

ドキュメントファイルを暗号化する暗号鍵を取得する手段と、上記ドキュメントファイルの印刷要件を指定する情報を上記ドキュメントファイルに関連付けてネットワークを介してサーバに登録する手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装された配布者端末と、

暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件をネットワークを介してサーバから取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えたことを特徴とするドキュメント保護システム。

【請求項 19】

ドキュメントファイルを暗号化する暗号鍵を取得する手段と、上記ドキュメントファイルの印刷要件を指定する情報を上記ドキュメントファイルに関連付けてネットワークを介してサーバに登録する手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装されたサーバと、

暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件をネットワークを介してサーバから取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えたことを特徴とするドキュメント保護システム。

【書類名】 明細書

【発明の名称】 ドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システム

【技術分野】**【0001】**

本発明はドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムに関する。

【背景技術】**【0002】**

近年、文書や画像などの情報（以下、ドキュメントという）を取り扱うオフィスなどにおいては、ドキュメントを紙に印刷する代わりにドキュメントファイルとして情報記録媒体へ電子的に記録しておく手法が主流となっている。

【0003】

ドキュメントを電子的に記録すれば、紙資源を用いることなくドキュメントを記録するため、省資源化を図れるとともに、ドキュメントが印刷された紙を格納する必要がなくなり、省スペース化を実現できる。

【0004】

また、ドキュメントを電子的に記録すれば、同一のドキュメントを多数人に対して同時に配布したり、遠隔地にいる者へネットワークを介してドキュメントを配布したりすることが可能となり、業務の効率化を図ることができる。

【0005】

同一のドキュメントを多数人に対して同時に配布したり、遠隔地にいる者へネットワークを介してドキュメントを配布できるというドキュメントを電子的に記録する場合の長所は、ドキュメントが漏洩しやすくなるという問題の裏返しでもある。

【0006】

オフィスなどにおいて取り扱われるドキュメントの中には、機密性を要するものも多数存在するため、ドキュメントの漏洩を防止するための対策を講じる必要がある。

【0007】

ドキュメントの漏洩を防止することを目的とした従来技術としては、特許文献1に開示される「Method of encrypting information for remote access while maintaining access control」、特許文献2に開示される「Information security architecture for encrypting documents for remote access while maintaining access control」、および、特許文献3に開示される「文書管理システム」のように、ドキュメントファイルを開く際にユーザ認証を求めて、正当なユーザだけがドキュメントの内容を参照できるようにする手法や、開いたドキュメントファイルを印刷しようとする際にユーザに印刷する権限があるか否かをチェックして権限があるユーザにのみ印刷させるものがある。

【0008】

また、特許文献4に開示される「電子的に伝送された情報の印刷制限方法および印刷制限付き文書」のように、支払いを済ませた場合にのみ印刷が許可されるようにドキュメントファイルをコントロールするような技術もある。

【特許文献1】 米国特許第6339825号明細書

【特許文献2】 米国特許第6289450号明細書

【特許文献3】 特開2001-142874号公報

【特許文献4】 特開2002-024097号公報

【発明の開示】**【発明が解決しようとする課題】****【0009】**

上記各特許文献に開示される発明においては、権限のない者がドキュメントを印刷できないように設定できるものの、印刷した物（プリントアウト）に対するセキュリティは何ら設定されていない。

【0010】

よって、印刷する権限を有するユーザになりすまして一度ドキュメントを印刷してしまえば、その後は何の制約を受けることなくドキュメントのプリントアウトを複製して他者に配布できることになる。

【0011】

さらに、ドキュメントを漏洩させようとする者が印刷する権限を有する正当なユーザである場合は、これを阻止することはできない。

【0012】

このように、従来の技術では、ドキュメントファイルの使い勝手が良くないとともに、プリントアウトによるドキュメントの漏洩を防止するためのセキュリティが不十分であるという問題があった。

【0013】

本発明はかかる問題に鑑みてなされたものであり、プリントアウトによるドキュメントの漏洩を防止したドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムを提供することを目的とする。

【課題を解決するための手段】**【0014】**

上記の目的を達成するため、本発明のドキュメント印刷プログラムは、暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件をネットワークを介してサーバから取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とを備えるようにしている。

【0015】

これにより、印刷時におけるセキュリティ対策を強制することができる。

【0016】

また、本発明のドキュメント保護プログラムは、ドキュメントファイルを暗号化する暗号鍵を取得する手段と、上記ドキュメントファイルの印刷要件を指定する情報を上記ドキュメントファイルに関連付けてネットワークを介してサーバに登録する手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とを備えるものとして構成できる。

【0017】

また、本発明のドキュメント保護システムは、ドキュメントファイルを暗号化する暗号鍵を取得する手段と、上記ドキュメントファイルの印刷要件を指定する情報を上記ドキュメントファイルに関連付けてネットワークを介してサーバに登録する手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装された配布者端末と、暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件をネットワークを介してサーバから取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えるものとして構成できる。

【0018】

また、ドキュメントファイルを暗号化する暗号鍵を取得する手段と、上記ドキュメントファイルの印刷要件を指定する情報を上記ドキュメントファイルに関連付けてネットワークを介してサーバに登録する手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装されたサーバと、暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件をネットワークを介してサーバから取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えるものとしても構成できる。

【発明の効果】

【0019】

本発明によれば、プリントアウトによるドキュメントの漏洩を防止したドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムを提供できる。

【発明を実施するための最良の形態】

【0020】

〔第1の実施形態〕

本発明を好適に実施した第1の実施形態について説明する。

【0021】

なお、本願発明者らは別途、配布者がドキュメントファイルに対してACL (Access Control List) を個々に設定することによりドキュメントファイルを保護する技術を提案しているが、多数のユーザにドキュメントを配布しようとする場合は、各ユーザごとに印刷要件を個別に設定することはドキュメントファイルの配布者がACLを作成するための負担が大きくなってしまう。

【0022】

一方、ドキュメントファイルの内容がビジネス文書などである場合は、これをどのように保護するかは、配布者が独自に決定するのではなく、所属する組織（企業や団体など）のセキュリティポリシー（秘密管理規則）に基づいて決定することとなる。よって、ドキュメント保護・印刷システムが配布者の所属する組織のセキュリティーポリシーに従ってドキュメントファイルを保護できれば、配布者がACLを設定しなくても良くなる。

【0023】

本発明の第1の実施形態では、配布者の所属する組織のセキュリティーポリシーに従ってドキュメントを保護するドキュメント保護・印刷システムについて説明する。

【0024】

図1に、本実施形態にかかるドキュメント保護・印刷システムの構成を示す。

【0025】

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末301、ユーザ端末302、プリンタ303およびアクセスコントロールサーバ304を有する。

【0026】

配布者端末301およびユーザ端末302は、表示装置（例えば、LCD）、入力装置（例えば、キーボード）、外部記録装置（例えば、FDD、HDD）などを備えたコンピュータ端末を適用できる。なお、配布者端末301にはドキュメント保護プログラム311が、ユーザ端末302にはドキュメント印刷プログラム321がそれぞれ実装されている。

【0027】

ドキュメント保護プログラム311は、ドキュメントファイルに配布者端末301の使用者（配布者）の入力操作に応じて印刷要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEAなど）を用いてドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。図2はドキュメント保護プログラム311の構成例を示したものであり、暗号化部311aと暗号鍵取得部311bと属性付与部311cと属性登録部311dとを含んでいる。各部の機能については後の動作において説明する。

【0028】

図1に戻り、ドキュメント印刷プログラム321は、ユーザ端末302の使用者（ユーザ）の入力操作に応じ、保護ドキュメントを復号するとともに設定されている印刷要件に応じた印刷処理をプリンタ303に実行させる処理を行うプログラムである。図3はドキュメント印刷プログラム321の構成例を示したものであり、復号部321aと復号鍵取得部321bと印刷要件取得部321cと印刷処理部321dとを含んでいる。また、図4は図3における印刷処理部321dの構成例を示したものであり、要件処理部321eとドキュメント加工部321fとプリンタドライバ321gと警告表示部321hとログ

記録部 321 i とを含んでいる。各部の機能については後の動作において説明する。

【0029】

図 1 に戻り、アクセスコントロールサーバ 304 は、ユーザがドキュメントにアクセス（例えば、印刷）しようとする場合に、ドキュメント印刷プログラム 321 からの要求に応じて ACL を参照し、ドキュメントにアクセスする権限があるか否か、処理要件がどのように設定されているかを取得するサーバである。

【0030】

アクセスコントロールサーバ 304 には、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）およびユーザの階級を示す情報が格納されたユーザデータベース 341 と、ユーザ各人ごとに設定された処理要件を含む ACL がセキュリティ属性に応じて複数登録されている ACL データベース 342 と、各保護ドキュメントにどのようなセキュリティ属性が設定されているかを示す情報およびその保護ドキュメントを復号するための暗号鍵が関連付けられて登録されるセキュリティ属性データベース 343 とが接続されている。

【0031】

図 5 はアクセスコントロールサーバ 304 の構成例を示したものであり、属性 DB 登録部 304 a とユーザ認証部 304 b とアクセス権限確認部 304 c と印刷要件取得送付部 304 d とを含んでいる。各部の機能については後の動作において説明する。

【0032】

なお、セキュリティ属性に応じた ACL の例をあげると、「第一設計室用 ACL」、「第二設計室用 ACL」のように小組織に応じた ACL である。ACL の構造例を図 6 に示すが、ACL はユーザ名（User Name）、アクセスタイプ（Access Type）、許可情報（Permission）および処理要件（Requirement）をパラメータとして構成される。そして、この ACL は、ACL データベース 342 内ではセキュリティ属性ごとに登録されている。

【0033】

なお、配布者の入力操作に応じてドキュメント保護プログラム 311 がドキュメントファイルに設定する印刷要件の例としては、地紋印刷（Background Dot Pattern：以下、BDP という）、機密印刷（Private Access：以下、PAC という）、電子透かし（Digital Watermark：以下、DWM という）の付加、バーコード付加（Embedding Barcode：以下、EBC という）、機密ラベルスタンプ（Security Label Stamp：以下、SLS という）などが挙げられる。

【0034】

本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。最初にシステム全体の動作について説明する。

【0035】

配布者は、配布者端末 301 を操作してこれにドキュメントファイルを実装しておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。

【0036】

ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末 301 の入力装置を操作してドキュメントファイルをドキュメント保護プログラム 311 に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム 311 は、セキュリティ属性の設定を配布者に要求する。例えば、ドキュメント保護プログラム 311 は、配布者端末 301 の表示装置にメッセージを表示するなどして、セキュリティ属性の設定を要求する。図 7 はセキュリティ属性の設定を要求する画面の例を示したものであり、文書カテゴリ（技術関連、人事関連等）および機密レベル（極秘、秘、社外秘、公開等）の設定がプルダウンメニュー等から選択することにより行えるようになっている。なお、図 7 の画面では保護するドキュメントファイルを指定することもできるようになっている。

【0037】

配布者が配布者端末 301 の入力装置を介してドキュメントファイルにセキュリティ属

性を設定すると、ドキュメント保護プログラム 311 はこれを取得する。

【0038】

セキュリティ属性を取得したドキュメント保護プログラム 311 は、ドキュメントファイルごとに固有のドキュメント ID を生成し、暗号化および復号に使用する暗号鍵とセキュリティ属性とをこれに関連付けてアクセスコントロールサーバ 304 へ送信し、セキュリティ属性データベース 343 への登録を要求する。

【0039】

また、ドキュメント保護プログラム 311 は、暗号鍵を用いて暗号化したドキュメントファイルに対してドキュメント ID を付加して保護ドキュメントを生成する。

【0040】

配布者は、ドキュメント保護プログラム 311 が生成した保護ドキュメントをユーザに受け渡す。

【0041】

ユーザがドキュメントを印刷しようとする場合には、ユーザ端末 302 に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末に読み取らせても良いし、ユーザ端末 302 が配布者端末 301 と通信可能である場合には、通信網を介して配布者端末 301 から保護ドキュメントを取得するようにしてもよい。

【0042】

ユーザが、ユーザ端末 302 の入力装置を介してドキュメント印刷プログラム 321 に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム 321 は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム 321 は、ユーザ端末 302 の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。図 8 はユーザ名（ユーザ ID）とパスワードを要求する画面の例を示したものであり、キーボード等によって入力が行えるようになっている。

【0043】

ドキュメント印刷プログラム 321 は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ 304 へ送信して、ユーザ認証を要求する。

【0044】

アクセスコントロールサーバ 304 は、ドキュメント印刷プログラム 321 から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【0045】

ユーザを特定すると、アクセスコントロールサーバ 304 は、セキュリティ属性データベース 343 を参照し、保護ドキュメントに設定されているセキュリティ属性の種類を特定する。その後、アクセスコントロールサーバ 304 は、ACL データベース 342 に登録されている ACL のうち、保護ドキュメントに設定されているセキュリティ属性に該当するものを参照し、ドキュメントファイルを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際には、どのような印刷要件が設定されているかを取得する。

【0046】

ユーザにドキュメントファイルを印刷する権限がある場合、アクセスコントロールサーバ 304 は、印刷が許可されていることを示す許可情報とともに、保護ドキュメントを復号するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とをユーザ端末 302 へ送信し、ドキュメント印刷プログラム 321 に受け渡す。

【0047】

アクセスコントロールサーバ 304 から許可情報とともに、暗号鍵と印刷要件とを取得したドキュメント印刷プログラム 321 は、暗号鍵を用いて保護ドキュメントを復号してドキュメントファイルに復元する。

【0048】

そしてドキュメント印刷プログラム 3 2 1 は、印刷要件を満たすようにプリンタ 3 0 3 に印刷処理を実行させる。例えば、ドキュメントファイルに前述した B D P が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【 0 0 4 9 】

これにより、ドキュメントファイルを印刷する際に、予め設定されたセキュリティ属性に応じた印刷要件を強制することが可能となる。

【 0 0 5 0 】

なお、ユーザが印刷要件について意識していない場合があると共に、印刷要件によっては特定のプリンタでないと処理できないものもあるため、印刷の実行前にその旨の情報がユーザに提供されることが望ましい。図 9 はユーザ端末 3 0 2 の表示装置上に表示される確認画面の例を示したものであり、印刷要件と利用できるプリンタとが表示され、使用するプリンタを選択することができるようになっている。

【 0 0 5 1 】

ここで、ドキュメントを保護する際のドキュメント保護プログラム 3 1 1 およびアクセスコントロールサーバ 3 0 4 の動作、および保護ドキュメントをドキュメントファイルに復元して印刷する際のドキュメント印刷プログラム 3 2 1 およびアクセスコントロールサーバ 3 0 4 の動作についてさらに詳しく説明する。

【 0 0 5 2 】

図 1 0 に、ドキュメント保護プログラム 3 1 1 が保護ドキュメントを生成する際の動作を示す。ドキュメント保護プログラム 3 1 1 は、配布者端末 3 0 1 の入力装置における配布者の入力操作によってドキュメントファイルとそのセキュリティ属性とを取得すると、ドキュメントファイルを暗号化および復号するための暗号鍵を生成する。そして、ドキュメント保護プログラム 3 1 1 は、生成した暗号鍵を用いてドキュメントファイルを暗号化し、暗号化ドキュメントを生成する。

【 0 0 5 3 】

さらにドキュメント保護プログラム 3 1 1 は、ドキュメントファイルごとに固有のドキュメント ID を暗号化ドキュメントに添付して保護ドキュメントを生成する。

【 0 0 5 4 】

保護ドキュメントを生成した後、ドキュメント保護プログラム 3 1 1 は配布者端末 3 0 1 の通信機能を用いて、暗号鍵とセキュリティ属性とドキュメント ID とをアクセスコントロールサーバ 3 0 4 へ送信し、これらの登録をアクセスコントロールサーバ 3 0 4 に要求する。

【 0 0 5 5 】

暗号鍵とセキュリティ属性とドキュメント ID とをドキュメント保護プログラム 3 1 1 から受け渡されたアクセスコントロールサーバ 3 0 4 は、これらに関連付けて一つのレコードとしてセキュリティ属性データベース 3 4 3 に登録し、記録保持する。

【 0 0 5 6 】

上記の動作を図 2 および図 5 に基づいてさらに詳しく説明する。

【 0 0 5 7 】

まず、図 2 において、ドキュメント保護プログラム 3 1 1 の暗号化部 3 1 1 a は、配布者から引き渡されたドキュメントファイルに対し、暗号鍵取得部 3 1 1 b が生成した暗号鍵を用いて暗号化を行い、この暗号化ドキュメントを属性付与部 3 1 1 c に渡す。

【 0 0 5 8 】

属性付与部 3 1 1 c はドキュメント ID を生成し、暗号化部 3 1 1 a から渡された暗号化ドキュメントにドキュメント ID を付与して保護ドキュメントとして出力する。

【 0 0 5 9 】

また、属性登録部 3 1 1 d は配布者からセキュリティ属性を受け取るとともに、暗号鍵取得部 3 1 1 b から暗号鍵を、属性付与部 3 1 1 c からドキュメント ID をそれぞれ受け取り、アクセスコントロールサーバ 3 0 4 に対してこれらのドキュメント ID、暗号鍵、セキュリティ属性を渡して登録を要求する。

【0060】

次いで、図5において、アクセスコントロールサーバ304の属性DB登録部304aは、渡されたドキュメントID、暗号鍵、セキュリティ属性をセキュリティ属性データベース343に登録する。

【0061】

なお、上記の例においてはドキュメントIDの生成や暗号鍵の生成をドキュメント保護プログラム311が行う場合を示したが、これらの処理はアクセスコントロールサーバ304や不図示のサーバなどで行っても良い。

【0062】

また、配布者端末301とアクセスコントロールサーバ304との間が専用回線ではなくネットワーク網を介して接続されており、暗号鍵など送信する際に盗聴される懸念がある場合には、SSL (Secure Socket Layer) を用いて通信を行えばよい。

【0063】

ドキュメント保護プログラム311がアクセスコントロールサーバ304と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Java (R) RMI (Remote Method Invocation) やSOAP (Simple Object Access Protocol) をベースとして情報を送受信するようにしても良い。その場合、アクセスコントロールサーバ304は、例えば「register(String docId, byte[] key, byte[] acl)」のようなメソッドを実装するようにしてもよい。SOAPであれば、HTTPSの上でSOAPプロトコルをやりとりし、RMIであればSSLベースのSocketFactoryを用いてRMIを実行するようにすれば、ネットワーク上でのセキュリティを確保することができる。

【0064】

次に、ドキュメント印刷プログラム321が保護ドキュメントを印刷する際の動作について説明する。

【0065】

図11に、ドキュメント印刷プログラム321が行う処理の内容を示す。また、図12に、ドキュメント印刷プログラム321およびアクセスコントロールサーバ304の動作の流れを示す。

【0066】

ドキュメント印刷プログラム321は、ユーザ端末302の入力装置におけるユーザの入力操作によって保護ドキュメントとユーザ名とパスワードとを取得すると、保護ドキュメントに添付されているドキュメントIDを取得する。

【0067】

そして、ユーザ名とパスワードとドキュメントIDとアクセスタイプ（ユーザが要求する処理を示す情報。ここでは、保護ドキュメントを印刷しようとするので、“print”となる。）とをアクセスコントロールサーバ304へ送信して、アクセス権限があるか否かのチェックを要求する。なお、図13はアクセスコントロールサーバ304へのSOAPによる問い合わせの例を示す図であり、ユーザ名（userId）とドキュメントID（docId）とアクセスタイプ（accessType）とを渡してアクセスが許可されているかを問い合わせるSOAPメッセージ（isAllowed）を送付し、その結果（isAllowedResponse）を受け取っている例である。結果には、許可されているということ（allowedがtrue）と要件（requirements）とが含まれている。

【0068】

アクセスコントロールサーバ304は、ドキュメント印刷プログラム321からユーザ名とパスワードとドキュメントIDとアクセスタイプとを取得すると、ユーザデータベース341に登録されている情報を参照し、ユーザ認証を行う。換言すると、アクセスコントロールサーバ304は、ユーザデータベース341に登録されている情報を参照し、ドキュメント印刷プログラム321から取得した情報に含まれるユーザ名とパスワードとの組と一致するものが、ユーザデータベース341に登録されているか否かを判断する。

【0069】

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム 3 2 1 から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース 3 4 1 に登録されていない場合）、アクセスコントロールサーバ 3 0 4 は、許可情報（ユーザが要求する処理を許可するか否かを示す情報）を「不許可」としてユーザ端末 3 0 2 へ送信し、ドキュメント印刷プログラム 3 2 1 へ受け渡す。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム 3 2 1 へ受け渡すようにしてもよい。

【0070】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ 3 0 4 は、セキュリティ属性データベース 3 4 3 に登録されているレコードのうち、ドキュメント印刷プログラム 3 2 1 から取得した情報に含まれるドキュメント ID に関するレコードを読み出す。

【0071】

アクセスコントロールサーバ 3 0 4 は、読み出したレコードに含まれるセキュリティ属性を取得する。そして、アクセスコントロールサーバ 3 0 4 は、ACL データベース 3 4 2 に登録されている ACL のうち、レコードから取得したセキュリティ属性に応じた ACL を読み出して取得する。さらに、アクセスコントロールサーバ 3 0 4 は、ドキュメント印刷プログラム 3 2 1 から取得したユーザ名およびアクセスタイプに基づいて、ACL から許可情報および印刷要件を取得する。

【0072】

換言すると、アクセスコントロールサーバ 3 0 4 は、ユーザ名とアクセスタイプとに基づいて、予め ACL に設定されている許可情報と印刷要件とを取得する。

【0073】

ACL から取得した許可情報が「許可」である場合、アクセスコントロールサーバ 3 0 4 は、レコードに格納されている暗号鍵と印刷要件とを許可情報とともにユーザ端末 3 0 2 へ送信してドキュメント印刷プログラム 3 2 1 に受け渡す。

【0074】

一方、ACL から取得した許可情報が「不許可」である場合、アクセスコントロールサーバ 3 0 4 は、許可情報のみをユーザ端末 3 0 2 へ送信してドキュメント印刷プログラム 3 2 1 に受け渡す。

【0075】

アクセスコントロールサーバ 3 0 4 から許可情報を受け渡されたドキュメント印刷プログラム 3 2 1 は、取得した許可情報を参照し、「不許可」である場合には、表示装置にメッセージを表示するなどして、要求された処理を実行できないことをユーザに通知する。

【0076】

一方、取得した許可情報が「許可」である場合には、許可情報と共に受け渡された暗号鍵を用いて、保護ドキュメントのうちの暗号化ドキュメントの部分を復号してドキュメントファイルに復元する。

【0077】

また、ドキュメント印刷プログラム 3 2 1 は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、PAC が指定されていれば機密印刷モードに設定する）、プリンタ 3 0 3 にドキュメントの印刷処理を実行させる。

【0078】

なお、必要があれば、表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【0079】

アクセスコントロールサーバ 3 0 4 から取得した印刷要件を満足する印刷をプリンタ 3 0 3 では実行できない場合、換言すると、プリンタ 3 0 3 が ACL に設定されていた印刷要件を満たす機能を備えていない場合には、ドキュメント印刷プログラム 3 2 1 は、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【0080】

上記の動作を図3～図5に基づいてさらに詳しく説明する。

【0081】

まず、図3において、ドキュメント印刷プログラム321の復号鍵取得部321bはアクセスコントロールサーバ304に対してアクセス権の確認を行う。

【0082】

確認の問い合わせを受けたアクセスコントロールサーバ304は、図5において、ユーザ認証部304bがユーザデータベース341を参照してユーザ認証を行い、認証結果をドキュメント印刷プログラム321に通知する。また、ユーザ認証に成功した場合、アクセス権限確認部304cがセキュリティ属性データベース343およびACLデータベース342を参照して許可情報および復号鍵を取得するとともに、印刷要件取得送付部304dがACLデータベース342から印刷要件を取得し、ドキュメント印刷プログラム321に通知する。なお、図5ではいったん認証結果を返してから再び認証結果を渡すようにしているが、これを一度に実行してもよい。また、許可情報、復号鍵および印刷要件を別々に返すようにしているが、これらを一度に返すようにしてもよい。

【0083】

図3において、復号鍵取得部321bはアクセス権の確認ができた場合にアクセスコントロールサーバ304から復号鍵を得て、これを復号部321aに渡す。また、印刷要件取得部321cはアクセスコントロールサーバ304から印刷要件を取得し、印刷処理部321dに渡す。

【0084】

復号部321aは復号鍵取得部321bから取得した復号鍵を用いて保護ドキュメントを復号し、ドキュメントファイルを得て印刷処理部321dに渡す。

【0085】

次いで、図4において、印刷処理部321dの要件処理部321eは、受け取った印刷要件の内容に応じて複数の処理を行う。すなわち、前述したBDP、EBC、SLSのようにドキュメントファイルそのものを加工する必要がある処理についてはドキュメント加工部321fに加工情報を与えてドキュメントファイルの加工を行わせ、加工済みのドキュメントファイルをプリンタドライバ321gに渡し、印刷データをプリンタ303に与えて印刷を行う。また、PACのようにプリンタドライバに特別な設定を行う必要がある処理についてはプリンタドライバ321gに印刷設定を行う。さらに、ユーザに対して警告メッセージを表示する必要がある場合には警告表示部321hに警告メッセージを渡し、表示装置に表示を行わせる。また、印刷のログを残す必要がある場合にはログ記録部321iにログ情報を渡し、リモートサーバ等にログデータを登録させる。

【0086】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、サーバ側でドキュメントファイルに対するアクセス権限を判断するシステム構成においては、ACLデータベース342に登録されているACLの内容を配布者端末301やアクセスコントロールサーバ304における入力操作によって変更できるようにしてもよく、この場合には、保護ドキュメントを配布した後で印刷要件を変更したりすることが可能となる。

【0087】

例えば、既に配布した保護ドキュメントに対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【0088】

なお、本実施形態にかかるドキュメント保護・印刷システムが上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム321に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメントを復号することも可能ではある。この場合は、ACLとして設定されている印刷要件を強制されることなく、保護ドキュメントを印刷できてしまうこととなる。

【0089】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム 311 の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。この場合は、ドキュメント印刷プログラム 321 にも同一の秘密鍵を埋め込んでおくことで、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム 321 のみが、保護ドキュメントを復号して印刷することが可能となる。

【0090】

図 14 および図 15 は上述したような内部に秘密鍵を埋め込んでおくタイプの構成例を示したものであり、図 14 はドキュメント保護プログラム 311 の構成例を示し、図 15 はドキュメント印刷プログラム 321 の構成例のうち復号に関する部分のみを示している。なお、この例は、単に内部に秘密鍵を埋め込んでおくだけではなく、乱数を導入して不正アクセスに対しより強化している。

【0091】

図 14 において、ドキュメント保護プログラム 311 は暗号化部 311a と暗号鍵取得部 311b と属性付与部 311c と属性登録部 311d とパラメータ取得部 311e とを含んでいる。

【0092】

動作にあつては、パラメータ取得部 311e はパラメータ (kp) を生成し、暗号鍵取得部 311b に渡す。なお、パラメータ (kp) はドキュメント保護プログラム 311 の内部に保持しておくか、要求があつた場合に生成するようにする。

【0093】

暗号鍵取得部 311b はパラメータ取得部 311e からパラメータ (kp) を受け取った上で、二つの乱数 (kd) (ks) を生成し、暗号鍵 (k) を式 $k = H\{ks, kp, kd\}$ あるいは $k = D\{kd, D\{ks, kp\}\}$ で計算して生成し、暗号鍵 (k) を暗号化部 311a に、乱数 (kd) を属性付与部 311c に、乱数 (ks) を属性登録部 311d にそれぞれ渡す。なお、 $H\{data1, data2, \dots\}$ は $data1, data2, \dots$ のハッシュ値を計算することを意味し、 $D\{data, key\}$ は key で data を復号することを意味している。

【0094】

暗号化部 311a は配布者から引き渡されたドキュメントファイル (doc) に対し、暗号鍵取得部 311b から取得した暗号鍵 (k) を用いて暗号化を行い、暗号化されたドキュメント (enc) を属性付与部 311c に渡す。式で示せば $enc = E\{doc, k\}$ となる。なお、 $E\{data, key\}$ は key で data を暗号化することを意味している。

【0095】

次いで、属性付与部 311c はドキュメント ID (id) を生成し、暗号化されたドキュメント (enc) にそのドキュメント ID (id) と暗号鍵取得部 311b から渡された乱数 (kd) を付与して保護ドキュメント ($enc + id + kd$) を出力する。また、属性付与部 311c は生成したドキュメント ID (id) を属性登録部 311d に渡す。

【0096】

属性登録部 311d は、属性付与部 311c から渡されたドキュメント ID (id) と暗号鍵取得部 311b から渡された乱数 (ks) と配布者から取得したセキュリティ属性 (atr) とをアクセスコントロールサーバ 304 に通知し、登録を要求することになる。

【0097】

復号にあつては、図 15 において、復号鍵取得部 321b は保護ドキュメントから乱数 (kd) を取得するとともに、パラメータ取得部 321j からドキュメント印刷プログラム 321 の内部に保持してある、あるいは要求に応じて生成したパラメータ (kp) を取得し、さらにアクセスコントロールサーバ 304 から乱数 (ks) を取得し、暗号化の場合と同様に式 $k = H\{ks, kp, kd\}$ あるいは $k = D\{kd, D\{ks, kp\}\}$ で計算して復号鍵（暗号鍵）(k) を得る。

【0098】

そして、復号部 321a は暗号化されたドキュメント (enc) を復号鍵 (k) で復号し、ドキュメントファイル (doc) を得る。

【0099】

図 14 および図 15 は、アクセスコントロールサーバ 304 に登録される乱数 (ks) と保護ドキュメント内の乱数 (kd) とドキュメント保護プログラム 311 もしくはドキュメント印刷プログラム 321 内から取得されるパラメータ (kp) とに基づいて暗号鍵 (復号鍵) (k) を生成する方式であるが、こうすることでアクセスコントロールサーバ 304 が悪意のあるユーザによって不正アクセスされて乱数 (ks) が知られてしまった場合であっても、乱数 (kd) やパラメータ (kp) が知られなければ保護ドキュメントを復号できないことになる。なお、アクセスコントロールサーバ 304 が不正アクセスされないように十分にガードされている環境にあつては、乱数 (ks) をそのまま暗号鍵 (復号鍵) (k) として使用してもよい。

【0100】

一方、これまで説明してきた第 1 の実施形態では、印刷要件をアクセスコントロールサーバ 304 にのみ格納するものとしてきたが、そのような形式に限定されず、保護ドキュメントに含めるようにしてもよい。例えば、ユーザによらずドキュメントファイルに対して必ず指定するような印刷要件については保護ドキュメントの中に含めるようにしてもよい。これは後述する第 2 の実施形態についても同様である。

【0101】

図 16 は、印刷要件を保護ドキュメントに含める第一印刷要件と、アクセスコントロールサーバ 304 に格納される第二印刷要件とに分けた場合のドキュメント印刷プログラム 321 の構成例を示したものであり、印刷要件取得部 321c においてアクセスコントロールサーバ 304 から第二印刷要件を取得するとともに、復号部 321a において保護ドキュメントから第一印刷要件を取得し、第一印刷要件および第二印刷要件に基づいて印刷処理部 321d で印刷処理を行うようにしている。その他は図 3 に示したドキュメント印刷プログラム 321 と同様である。

【0102】

また、本実施形態においては、ドキュメント印刷プログラム 321 は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム 321 は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat (R) の Plug-in としてポータブルドキュメントファイル (Portable Document Format: PDF File) の表示、編集および印刷の機能を実現することが可能である。

【0103】

このように、本実施形態にかかるドキュメント保護・印刷システムによれば、セキュリティ属性に応じて予め ACL として設定されている印刷要件を、ドキュメントファイルを印刷する際に強制することが可能となる。

【0104】

〔第 2 の実施形態〕

上記本発明の第 1 の実施形態においては、配布者の所属する組織のセキュリティポリシーに従ってドキュメントを保護するドキュメント保護・印刷システムについて説明した。

【0105】

しかし、第 1 の実施形態にかかるドキュメント保護・印刷システムは、配布者が所属する組織の規模が大きい場合は、その下位組織ごとに数多くの ACL を予め定義して登録しておかなければならない。例えば、「第一設計室の技術文書用 ACL」、「第一設計室の契約書用 ACL」、「第二設計室の技術文書用 ACL」、「第二設計室の契約書用 ACL」のように、各ユーザを網羅するように ACL を予め定義しておく必要がある。

【0106】

一般に、組織の掲げるセキュリティポリシーは総則的なものであり、誰にどのドキュメ

ントファイルに対するアクセスを許可するかといったことまでを規定するものではない。

【0107】

組織の掲げるセキュリティポリシーの例を図17に示す。図17に示すように、組織におけるセキュリティポリシーは、ドキュメントに対して機密レベル (Sensitivity) および分野 (Category) を設定した上で、ドキュメントに対するアクセスを許可するユーザの階級 (Level) や部門 (Category) およびその印刷要件を設定したものであるといえる。

【0108】

例えば、機密レベルが極秘 (Top Secret) の人事関連 (Human Resource) のドキュメントは、人事部の管理職のみが地紋印刷を条件として印刷可能という具合である。

【0109】

本発明の第2の実施形態では、組織の掲げるセキュリティポリシーをそのままの形で電子的に記述したものをドキュメントファイルの保護に適用したドキュメント保護・印刷システムについて説明する。

【0110】

図18に、本実施形態にかかるドキュメント保護・印刷システムの構成を示す。

【0111】

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末401、ユーザ端末402、プリンタ403およびアクセスコントロールサーバ404を有する。

【0112】

配布者端末401およびユーザ端末402は、第1の実施形態と同様に、表示装置 (例えば、LCD)、入力装置 (例えば、キーボード)、外部記録装置 (例えば、FDD、HDD)などを備えたコンピュータ端末を適用できる。なお、配布者端末401にはドキュメント保護プログラム411が、ユーザ端末402にはドキュメント印刷プログラム421がそれぞれ実装されている。

【0113】

ドキュメント保護プログラム411は、ドキュメントファイルに配布者端末401の使用者 (配布者) の入力操作に応じた処理要件を設定するとともに、暗号化アルゴリズム (RC4、Triple DES、IDEAなど) を用いてドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。ドキュメント保護プログラム411の内部構成は図2に示した第1の実施形態におけるものと同様である。

【0114】

ドキュメント印刷プログラム421は、ユーザ端末402の使用者 (ユーザ) の入力操作に応じ、保護ドキュメントを復号するとともに設定されている印刷要件に応じた印刷処理をプリンタ403に実行させる処理を行うプログラムである。ドキュメント印刷プログラム421の内部構成は図3および図4に示した第1の実施形態におけるものと同様である。

【0115】

アクセスコントロールサーバ404は、ユーザがドキュメントを印刷しようとする場合に、ドキュメント印刷プログラム421からの要求に応じて自身が記録保持しているセキュリティポリシー444を参照し、ドキュメントを印刷する権限があるか否か、印刷要件がどのように設定されているかを取得するサーバである。図19はアクセスコントロールサーバ404の構成例を示したものであり、属性DB登録部404aとユーザ認証部404bとアクセス権限確認部404cと印刷要件取得送付部404dとを含んでいる。各部の機能については後の動作において説明する。

【0116】

図20に、アクセスコントロールサーバ404に登録されるセキュリティポリシー444の例を示す。

【0117】

例えば、カテゴリが「技術 (Technical)」で機密レベルが「マル秘 (Secret)」のドキュメントファイルは、カテゴリが「技術 (Technical)」で階級が「中 (Medium)」又

は「上 (High)」のユーザに対して、閲覧は許可するがRADを要件とすること、印刷を許可するがPACとBDPとEBCとRADとを要件とすること、および、ハードコピーは許可しないことが規定されている。

【0118】

アクセスコントロールサーバ404は、セキュリティポリシー444のデータをどのような形で記録保持していても構わない。なお、XML (eXtensible Markup Language) を用いれば、図21に示すように、簡単に記述できる。

【0119】

アクセスコントロールサーバ404には、ユーザ各人の認証用の情報 (ユーザ名とパスワードとの組) が格納されたユーザデータベース441と、各保護ドキュメントにどのようなセキュリティ属性が設定されているかを示す情報およびその保護ドキュメントを復号するための暗号鍵が関連付けられて登録されるセキュリティ属性データベース443とが接続されている。

【0120】

図22に、ユーザデータベース441に登録される情報の例を示す。

【0121】

図22においてはユーザごとにカテゴリと階級とを別々の属性として管理する構造としているが、たとえば、Windows (R) Domainのユーザ管理機構を利用してユーザを管理するような場合には、グループアカウントとしてTechnical_Mediumのようなものを生成し、Ichiroというユーザをそのグループに所属させるようにしてもよい。所属グループの命名規則をこのように設定しておくことで、カテゴリと階級とを管理することが可能となる。

【0122】

本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。最初に、システム全体の動作について説明する。

【0123】

配布者は、配布者端末401を操作してこれにドキュメントファイルを実装しておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。

【0124】

ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末401の入力装置を操作してドキュメントファイルをドキュメント保護プログラム411に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム411は、セキュリティ属性の設定を配布者に要求する。例えば、ドキュメント保護プログラム411は、配布者端末401の表示装置にメッセージを表示するなどして、セキュリティ属性の設定を要求する。セキュリティ属性の設定を要求する画面は図7に示した第1の実施形態におけるものと同様である。なお、ここでのセキュリティ属性とは、保護しようとするドキュメントがセキュリティ属性データベース443に登録されているセキュリティ属性のうちのいずれに該当するかを示す情報である。

【0125】

配布者が配布者端末401の入力装置を介してドキュメントファイルにセキュリティ属性を設定すると、ドキュメント保護プログラム411はこれを取得する。

【0126】

セキュリティ属性を取得したドキュメント保護プログラム411は、ドキュメントファイルごとに固有のドキュメントIDを生成し、復号に使用する暗号鍵とセキュリティ属性とをこれに関連付けてアクセスコントロールサーバ404へ送信し、登録する。

【0127】

また、ドキュメント保護プログラム411は、暗号鍵を用いて暗号化したドキュメントファイルに対してドキュメントIDを付加して保護ドキュメントを生成する。

【0128】

配布者は、ドキュメント保護プログラム411が生成した保護ドキュメントをユーザに

受け渡す。

【0129】

ユーザがドキュメントを印刷しようとする場合には、ユーザ端末402に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末に読み取らせても良いし、ユーザ端末402が配布者端末401と通信可能である場合には、通信網を介して配布者端末401から保護ドキュメントを取得するようにしてもよい。

【0130】

ユーザが、ユーザ端末402の入力装置を介してドキュメント印刷プログラム421に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム421は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム421は、ユーザ端末402の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。ユーザ名とパスワードの入力をユーザに要求する画面は図8に示した第1の実施形態におけるものと同様である。

【0131】

ドキュメント印刷プログラム421は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ404へ送信して、ユーザ認証を要求する。

【0132】

アクセスコントロールサーバ404は、ドキュメント印刷プログラム421から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【0133】

ユーザを特定すると、アクセスコントロールサーバ404は、セキュリティ属性データベース443を参照し、保護ドキュメントに設定されているセキュリティ属性の種類を特定する。

【0134】

アクセスコントロールサーバ404は、ユーザデータベース441から取得したユーザの階級を示す情報および、ドキュメントに設定されているセキュリティ属性とに基づいて、ドキュメントを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際にはどのような印刷要件が設定されているのかを取得する。

【0135】

ユーザにドキュメントファイルを印刷する権限がある場合、アクセスコントロールサーバ404は、印刷が許可されていることを示す許可情報とともに、保護ドキュメントを復号するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とをユーザ端末402へ送信し、ドキュメント印刷プログラム421に受け渡す。

【0136】

アクセスコントロールサーバ404から許可情報とともに、暗号鍵と印刷要件とを取得したドキュメント印刷プログラム421は、暗号鍵を用いて保護ドキュメントを復号してドキュメントファイルに復元する。

【0137】

そしてドキュメント印刷プログラム421は、印刷要件を満たすようにプリンタ403に印刷処理を実行させる。例えば、ドキュメントファイルにBDPが印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【0138】

これにより、ドキュメントファイルを印刷する際に、予め設定されたセキュリティ属性に応じた印刷要件を強制することが可能となる。

【0139】

ここで、ドキュメントを保護する際のドキュメント保護プログラム411およびアクセスコントロールサーバ404の動作、および保護ドキュメントをドキュメントファイルに復元して印刷する際のドキュメント印刷プログラム421およびアクセスコントロールサーバ404の動作についてさらに詳しく説明する。

【0 1 4 0】

図 2 3 に、ドキュメント保護プログラム 4 1 1 が保護ドキュメントを生成する際の処理を示す。また、図 2 4 に、ドキュメント保護プログラム 4 1 1 およびアクセスコントロールサーバ 4 0 4 の動作の流れを示す。

【0 1 4 1】

ドキュメント保護プログラム 4 1 1 は、配布者端末 4 0 1 の入力装置における配布者の入力操作によってドキュメントファイルとそのセキュリティ属性とを取得すると、ドキュメントファイルを暗号化および復号するための暗号鍵を生成する。そして、ドキュメント保護プログラム 4 1 1 は、生成した暗号鍵を用いてドキュメントファイルを暗号化して、暗号化ドキュメントを生成する。

【0 1 4 2】

さらに、ドキュメント保護プログラム 4 1 1 は、ドキュメントファイルごとに固有のドキュメント ID を暗号化ドキュメントに添付して保護ドキュメントを生成する。

【0 1 4 3】

保護ドキュメントを生成した後、ドキュメント保護プログラム 4 1 1 は、配布者端末 4 0 1 の通信機能を用いて、暗号鍵とセキュリティ属性とドキュメント ID とをアクセスコントロールサーバ 4 0 4 へ送信し、これらの登録をアクセスコントロールサーバ 4 0 4 に要求する。

【0 1 4 4】

暗号鍵とセキュリティ属性とドキュメント ID とをドキュメント保護プログラム 4 1 1 から受け渡されたアクセスコントロールサーバ 4 0 4 は、これらを一つのレコードとしてセキュリティ属性データベース 4 4 3 に記録保持する。より詳しくは、図 1 9 におけるアクセスコントロールサーバ 4 0 4 の属性 DB 登録部 4 0 4 a がセキュリティ属性データベース 4 4 3 への登録を行う。

【0 1 4 5】

なお、ドキュメント保護プログラム 4 1 1 がドキュメント ID を生成して暗号化ドキュメントに添付する場合を例に挙げたが、SHA-1 などのハッシュアルゴリズムを用いて暗号化ドキュメントファイルを生成した場合には、そのハッシュ値をドキュメント ID の代わりに用いてもよい。この場合は、保護ドキュメントにドキュメント ID を添付する必要はなく、後でドキュメント ID を取得したい時は、再度ハッシュ値を計算すれば良い。

【0 1 4 6】

また、上記の例においてはドキュメント ID の生成や暗号鍵の生成をドキュメント保護プログラム 4 1 1 が行う場合を示したが、これらの処理はアクセスコントロールサーバ 4 0 4 や不図示のサーバなどで行っても良い。

【0 1 4 7】

また、配布者端末 4 0 1 とアクセスコントロールサーバ 4 0 4 との間が専用回線ではなくネットワーク網を介して接続されており、暗号鍵など送信する際に盗聴される懸念がある場合には、SSL (Secure Socket Layer) を用いて通信を行えばよい。

【0 1 4 8】

ドキュメント保護プログラム 4 1 1 がアクセスコントロールサーバ 4 0 4 と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Java (R) RMI (Remote Method Invocation) や SOAP (Simple Object Access Protocol) をベースとして情報を送受信するようにしても良い。その場合、アクセスコントロールサーバ 4 0 4 は、例えば「register(String docId, byte[] key, byte[] acl)」のようなメソッドを実装するようにしてもよい。SOAP であれば、HTTPS の上で SOAP プロトコルをやりとりし、RMI であれば SSL ベースの SocketFactory を用いて RMI を実行するようにすれば、ネットワーク上でのセキュリティを確保することができる。

【0 1 4 9】

次に、ドキュメント印刷プログラム 4 2 1 が保護ドキュメントを印刷する際の動作につ

いて説明する。図 2 5 に、ドキュメント印刷プログラム 4 2 1 およびアクセスコントロールサーバ 4 0 4 の動作の流れを示す。

【0 1 5 0】

ドキュメント印刷プログラム 4 2 1 は、ユーザ端末 4 0 2 の入力装置におけるユーザの入力操作によって保護ドキュメントとユーザ名とパスワードとを取得すると、保護ドキュメントに添付されているドキュメント ID を取得する。

【0 1 5 1】

そして、ユーザ名とパスワードとドキュメント ID とアクセスタイプ（ユーザが要求する処理を示す情報。ここでは、保護ドキュメントを印刷しようとするので、“print”となる。）とをアクセスコントロールサーバ 4 0 4 へ送信して、アクセス権限があるか否かのチェックを要求する。

【0 1 5 2】

アクセスコントロールサーバ 4 0 4 は、ドキュメント印刷プログラム 4 2 1 からユーザ名とパスワードとドキュメント ID とアクセスタイプとを取得すると、ユーザデータベース 4 4 1 に登録されている情報を参照し、ユーザ認証を行う。

【0 1 5 3】

換言すると、アクセスコントロールサーバ 4 0 4 は、ユーザデータベース 4 4 1 に登録されている情報を参照し、ドキュメント印刷プログラム 4 2 1 から取得した情報に含まれるユーザ名とパスワードとの組と一致するものが、ユーザデータベース 4 4 1 に登録されているか否かを判断する。

【0 1 5 4】

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム 4 2 1 から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース 4 4 1 に登録されていない場合）、アクセスコントロールサーバ 4 0 4 は、許可情報を「不許可」としてユーザ端末 4 0 2 へ送信し、ドキュメント印刷プログラム 4 2 1 へ受け渡す。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム 4 2 1 へ受け渡すようにしてもよい。

【0 1 5 5】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ 4 0 4 は、セキュリティ属性データベース 4 4 3 に登録されているレコードのうち、ドキュメント印刷プログラム 4 2 1 から取得した情報に含まれるドキュメント ID に関するレコードを読み出す。また、アクセスコントロールサーバ 4 0 4 は、ユーザデータベース 4 4 1 からユーザの「階級」および「部門」を取得する。

【0 1 5 6】

アクセスコントロールサーバ 4 0 4 は、読み出したレコードに基づいてドキュメントファイルに設定されているセキュリティ属性（すなわち、機密レベルおよびカテゴリ）を取得する。そして、自身が記録保持しているセキュリティポリシー 4 4 4 とレコードから読み出したセキュリティ属性に基づいて、ユーザがドキュメントに対してアクセスタイプで示される処理を行う場合の可否を示す許可情報とユーザがドキュメントを印刷する際の印刷要件を取得する。

【0 1 5 7】

ユーザにドキュメントファイルを印刷する権限がある場合は、セキュリティポリシー 4 4 4 として設定されている許可情報は「許可」であるため、アクセスコントロールサーバ 4 0 4 は、レコードに格納されていた暗号鍵と印刷要件とを許可情報とともにユーザ端末 4 0 2 へ送信して、ドキュメント印刷プログラム 4 2 1 に受け渡す。

【0 1 5 8】

一方、ユーザにドキュメントファイルを印刷する権限がない場合は、セキュリティポリシー 4 4 4 として設定されている許可情報は「不許可」であるため、アクセスコントロールサーバ 4 0 4 は、許可情報のみをユーザ端末 4 0 2 へ送信してドキュメント印刷プログラム 4 2 1 に受け渡す。

【0159】

上記のアクセスコントロールサーバ404における処理は、より詳しくは、図19に示すように、ユーザ認証部404bがユーザデータベース441を参照してユーザ認証を行い、認証結果をアクセス権限確認部404cに通知する。また、ユーザ認証に成功した場合、アクセス権限確認部404cがセキュリティ属性データベース443およびセキュリティポリシー444を参照して許可情報および復号鍵を取得するとともに、印刷要件取得送付部404dがセキュリティポリシー444から印刷要件を取得し、ドキュメント印刷プログラム421に通知する。なお、図19では許可情報、復号鍵および印刷要件を別々に返すようにしているが、これらを一度に返すようにしてもよい。

【0160】

次いで、ドキュメント印刷プログラム421は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、PACが指定されていれば機密印刷モードに設定する）、プリンタ403にドキュメントファイルの印刷処理を実行させる。

【0161】

なお、必要があれば、表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【0162】

アクセスコントロールサーバ404から取得した印刷要件を満足する印刷をプリンタ403では実行できない場合、換言すると、プリンタ403がセキュリティポリシー444として設定されていた印刷要件を満たす機能を備えていない場合には、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【0163】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、サーバ側でドキュメントファイルに対するアクセス権を判断するシステム構成においては、アクセスコントロールサーバ404に登録されているセキュリティポリシー444を配布者端末401やアクセスコントロールサーバ404における入力操作によって変更できるようにしてもよく、この場合には、保護ドキュメントを配布したあとで印刷要件を変更したりすることが可能となる。

【0164】

例えば、既に配布した保護ドキュメントに対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【0165】

なお、ドキュメントファイルを印刷する際に、ドキュメント印刷プログラム421が必ずアクセスコントロールサーバ404に対してセキュリティポリシーを問い合わせる方式とすると、ユーザ数の増加に伴いアクセスコントロールサーバ404の情報処理量が増え、負担が大きくなってしまう。

【0166】

このため、アクセスコントロールサーバ404の機能の一部をドキュメント印刷プログラム421に移行してもよい。

【0167】

例えば、ドキュメント印刷プログラム421は、ユーザ認証を行った上で、ドキュメントIDをアクセスコントロールサーバ404へ受け渡すと、セキュリティポリシーと暗号鍵とセキュリティ属性とをアクセスコントロールサーバ404から取得し、これを基に許可情報や印刷要件を判断して処理するようにしてもよい。

【0168】

このようにすれば、アクセスコントロールサーバ404の情報処理量を減らし、システム動作上の負担を軽減できる。この場合は、セキュリティポリシーに基づいた判断をドキュメント印刷プログラム421が行うため、ドキュメントにセキュリティ属性を添付した後に暗号化して暗号化ドキュメントとし、ドキュメントIDを添付して保護ドキュメント

とすることが好ましい。これにより、セキュリティ属性をアクセスコントロールサーバ 4 0 4 で管理する必要がなくなり、システム動作上のアクセスコントロールサーバ 4 0 4 の負担をさらに軽減できる。

【0169】

なお、本実施形態にかかるドキュメント保護・印刷システムが上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム 4 2 1 に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメントを復号することも可能ではある。この場合は、セキュリティポリシーとして設定されている印刷要件を強制されることなく、保護ドキュメントを印刷できてしまうこととなる。

【0170】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム 4 1 1 の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。この場合は、ドキュメント印刷プログラム 4 2 1 にも同一の秘密鍵を埋め込んでおくことで、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム 4 2 1 のみが、保護ドキュメントを復号して印刷することが可能となる。具体的には、第 1 の実施形態におけるものと同様に、図 1 4 および図 1 5 のように構成することができる。

【0171】

また、本実施形態においては、ドキュメント印刷プログラム 4 2 1 は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム 4 2 1 は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat (R) の Plug-in としてポータブルドキュメントファイル (Portable Document Format : P D F File) の表示、編集および印刷の機能を実現することが可能である。

【0172】

このように、本実施形態にかかるドキュメント保護・印刷システムによれば、予めセキュリティポリシーとして設定されている印刷要件をドキュメントを印刷する際に強制することができる。

【0173】

図 2 6 に、上記各実施形態において適用されるプリンタが備えるセキュリティ機能の一部を示す。これらについて第 2 の実施形態におけるシステム構成を例として具体的に説明する。

【0174】

まず、印刷要件として P A C が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。P A C が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作を図 2 7 に示す。

【0175】

(1) ドキュメント印刷プログラム 4 2 1 は P A C が設定されているドキュメントファイルを印刷する際には、図 2 8 に示すように、プリントダイアログを表示させた後に個人識別番号 (Personal Identification Number : P I N) を入力するダイアログをユーザ端末 4 0 2 の表示装置に表示させ、ユーザに P I N の入力を要求する。

【0176】

(2) ユーザ端末 4 0 2 の入力装置を用いてユーザが P I N を入力すると、ドキュメント印刷プログラム 4 2 1 は、これをプリンタドライバに設定し、印刷を指示する。

【0177】

プリンタドライバは、ドキュメントから Postscript などの P D L (Page Description Language) で記述された印刷データ (P D L データ) を生成し、印刷部数や出力トレイなどの印刷ジョブ情報を記述した P J L (Print Job Language) データを P D L データの先頭に付加する。プリンタドライバはさらに P J L データの一部として P I N を付加し、そ

の P J L データ付き P D L データをプリンタ 4 0 3 に送る。

【0178】

プリンタ 4 0 3 は、P J L データ付き P D L データを受け取ると P J L データの内容を参照し、機密印刷用の P I N が含まれている場合は印刷出力せずにプリンタ 4 0 3 内部の記憶装置（HDD など）に P J L データ付き P D L データを保存する。ユーザが P I N をプリンタ 4 0 3 のオペレーションパネルを介して入力すると、プリンタ 4 0 3 は入力された P I N を P J L データに含まれる P I N と照合し、一致すれば P J L データに含まれていた印刷ジョブ条件（部数、トレイなど）を適用しながら P D L データに従って印刷出力する。

【0179】

（3）プリンタドライバに P I N が設定できない、すなわち、プリンタ 4 0 3 が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。

【0180】

このようにすることで、印刷実行後、プリンタ 4 0 3 のオペレーションパネルにおいて印刷実行前に入力したものと同一の P I N が入力されるまでドキュメントのプリントアウトがプリンタ 4 0 3 から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ 4 0 3 に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ 4 0 3 とのやりとりを S S L で保護してもよい。

【0181】

また、ドキュメント印刷プログラム 4 2 1 を Windows（R）Domain のユーザ管理と連動させて、ユーザに対して P I N の入力を要求しないようにしてもよい。例えば、P I N をユーザに入力させるのではなく、Windows（R）Domain から現在ログオン中のユーザ I D を取得し、プリントデータとともにユーザ I D をプリンタ 4 0 3 へ送付するようにする。プリンタ 4 0 3 は、オペレーションパネルでユーザからのパスワード入力を受け、そのユーザ I D とパスワードとで Windows（R）Domain のユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。Windows（R）Domain に限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒な P I N 入力の手間を削減できる。

【0182】

次に、印刷要件として E B C が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。

【0183】

（1）ドキュメント印刷プログラム 4 2 1 は、E B C が設定されているドキュメントを印刷する際にドキュメント I D を示すバーコード画像データ（又は、二次元コード）のデータを生成する。

【0184】

（2）ドキュメント印刷プログラム 4 2 1 は、生成したバーコード画像データをスタンプ画像としてプリンタドライバにセットし、プリンタ 4 0 3 に印刷を指示する。

【0185】

（3）プリンタドライバに E B C が設定できない、すなわち、プリンタ 4 0 3 がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0186】

このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキャナのみがバーコードをデコードすることでドキュメント I D を取得し、そのドキュメント I D を基にアクセスコントロールサーバ 4 0 4 でハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキ

セキュリティ確保が可能となる。

【0187】

次に、印刷要件としてBDPが設定されている場合のドキュメント印刷プログラム421の動作について説明する。

【0188】

(1) ドキュメント印刷プログラム421は、BDPが設定されているドキュメントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する（例えば、Ichiro,2002/08/04 23:47:10）。

【0189】

(2) ドキュメント印刷プログラム421は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。

【0190】

(3) ドキュメント印刷プログラム421は、生成した地紋画像をスタンプとしてプリンタドライバにセットし、プリンタ403にドキュメントの印刷を指示する。

【0191】

(4) プリンタドライバにBDPが設定できない場合、すなわちプリンタ403が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0192】

このようにすることで、ドキュメントのプリントアウトの各ページには、印刷処理を実行したユーザ名と日時とが浮き出る地紋画像として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これ、EBCをサポートしていない複写機を使用する場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。

【0193】

次に、印刷要件としてSLSが設定されている場合のドキュメント印刷プログラム421の動作について説明する。

【0194】

(1) ドキュメント印刷プログラム421は、SLSが設定されているドキュメントファイルを印刷する際に、予め用意された画像のうち、そのドキュメントの機密レベルに応じたもの（Top Secretならば「極秘」のマークなど）を選択する。

【0195】

(2) 選択した画像のデータを、スタンプとしてプリンタドライバにセットし、プリンタ403に印刷を指示する。

【0196】

(3) プリンタドライバにSLSをセットできない場合、すなわち、プリンタ403がSLSをサポートしていない場合には、ラベルスタンプをサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0197】

このようにすることで、ドキュメントファイルのプリントアウトには、自動的に「極秘」や「マル秘」がスタンプとして印刷されるため、ドキュメントが機密文書であることが明らかとなる。すなわち、プリントアウトを所持する者に管理上の注意を喚起することができる。

【0198】

上記の各例は、あくまでも印刷要件の例であり、改ざん防止用の電子透かしを印刷するようにしたり、保護されているドキュメントは特殊な用紙に印刷する（印刷に使用する用紙トレイを特殊用紙のトレイに限定する）ようにしてもよい。

【0199】

さらに付言すると、印刷要件には、機能を制限・禁止するものと、機能を強制的に使用させるもの、加えて通常の印刷条件指定などを含めることができる。機能を制限・禁止す

る例としては、機密文書原本と区別をするために特別なユーザのみカラーでの印刷を許可して、他のユーザはグレースケールでの印刷のみを許可するように制限するための印刷要件などである。機能を強制的に使用させる例としては、機密印刷モードを強制的に使用するような印刷要件や、ログを強制的に記録するような印刷要件、印刷紙面に印刷したユーザの名前を強制的に印字するような印刷要件、ウォーターマークを強制的に印刷する印刷要件、地紋を強制的に印刷する印刷要件などである。通常の印刷条件を指定する例としては、用紙設定としてA4を指定する印刷要件、再生紙トレイを使用する印刷要件、両面印刷を指定する印刷要件などである。

【0200】

また、これまで印刷要件の表現形式としてRAD、PACといったキーワードを用いて説明してきたが、そのようなキーワードでなくとも、例えば、プリンタドライバに設定する設定ファイルのデータそのものや、プリントデータに挿入するページ記述言語で表現したデータ、画面に表示する文字列そのもの、処理すべき要件の内容をスクリプト言語で記述したデータのようなものを用いて印刷要件を表現して規定するようにしても良い。すなわち、印刷要件の表現をキーワードのようなものに限定するものではない。

【0201】

このように、プリンタ403がサポートする様々なセキュリティ機能を利用してセキュリティポリシーに沿った印刷要件を設定することによって、プリンタ403のセキュリティ機能が無駄なく活用して、プリントアウトに至るまで一貫したセキュリティの確保が可能となる。これは他の実施形態のシステム構成においても同様である。

【0202】

一方、これまでの説明において、保護対象はドキュメント全体であるように記述してきたが、ドキュメントの中に保護対象となる部分（セグメントと呼ぶ）と、保護対象としない部分が混在していても良い。例えば、図29に示すように、保護セグメントが複数保護ドキュメント内に存在していても良い。この場合、保護セグメントごとに異なるセグメントIDをつけ、これまでの説明におけるドキュメントIDをセグメントIDと読みかえれば、同じ原理で保護セグメントごとに印刷を含むアクセスの制御が可能になる。実際には、保護セグメントの先頭と末尾には、そこから保護セグメントが開始することを示しそこで保護セグメントが終了することを示すマークのようなものをつける必要がある。そういったマークの入れ方については、MIMEのマルチパートセパレータなどの従来技術を用いることができる。

【0203】

また、これまではドキュメント保護プログラムが配布者端末に配置されるような実施例に基づいて説明してきたが、ドキュメント保護プログラム本体はリモートサーバ上に配置するようにしても良い。例えば図18の配布者端末401、ドキュメント保護プログラム411およびアクセスコントロールサーバ404の関係は、図30に示すように変形することができる。このように配置することにより、ドキュメント保護プログラムがインストールされていない端末からでもリモートサーバにドキュメントと必要なパラメータを送付して保護ドキュメントを取得することができる。

【0204】

なお、上述した各実施形態は、本発明の好適な実施の例であり、本発明はこれらに限定されることはない。

【0205】

例えば、上記各実施形態においては、配布者端末とユーザ端末とが別個の装置である場合を例に説明を行ったが、これらは同一の装置を共用するような構成であっても構わない。

【0206】

また、上記各実施形態では、ドキュメント印刷プログラムが実装されたユーザ端末を、ユーザが直接操作する場合を例に説明を行ったが、これに限定されるものではない。例えば、ドキュメント印刷プログラムがサーバに実装されており、ユーザがユーザ端末を操作

しネットワーク網を介してドキュメント印刷プログラムを実行させる構成であってもよい。

【0207】

また、ユーザ認証の方法は、ユーザ名とパスワードとを用いる方法に限定されることはなく、スマートカードを用いたPKIベースの認証方法を適用してもよい。

【0208】

このように、本発明は様々な変形が可能である。

【0209】

さらに、上記の説明では「プリンタ」という用語が使われているが、これは狭義のプリンタ専用機に限らず、コピー、ファクシミリ、これらの複合・融合された機器等、すなわち印刷機能を有するすべての機器を意味するものである。

【図面の簡単な説明】

【0210】

【図1】 本発明を好適に実施した第1の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。

【図2】 ドキュメント保護プログラムの構成例を示す図である。

【図3】 ドキュメント印刷プログラムの構成例を示す図である。

【図4】 印刷処理部の構成例を示す図である。

【図5】 アクセスコントロールサーバの構成例を示す図である。

【図6】 ACLの構成例を示す図である。

【図7】 セキュリティ属性の設定を要求する画面の例を示す図である。

【図8】 ユーザ名（ユーザID）とパスワードを要求する画面の例を示す図である。

【図9】 ユーザ端末の表示装置上に表示される確認画面の例を示す図である。

【図10】 第1の実施形態にかかるドキュメント保護プログラムおよびアクセスコントロールサーバの動作の流れを示す図である。

【図11】 第1の実施形態にかかるドキュメント印刷プログラムの動作を示す図である。

【図12】 第1の実施形態にかかるドキュメント印刷プログラムおよびアクセスコントロールサーバの動作の流れを示す図である。

【図13】 アクセスコントロールサーバへのSOAPによる問い合わせの例を示す図である。

【図14】 ドキュメント保護プログラムの構成例を示す図である。

【図15】 復号の様子を示す図である。

【図16】 ドキュメント印刷プログラムの構成例を示す図である。

【図17】 セキュリティポリシーの例を示す図である。

【図18】 本発明を好適に実施した第2の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。

【図19】 アクセスコントロールサーバの構成例を示す図である。

【図20】 セキュリティポリシーを電子データとした場合のデータ構造を示す図である。

【図21】 セキュリティポリシーを電子データとして記述した例を示す図である。

【図22】 ユーザデータベースに記録される情報の構造例を示す図である。

【図23】 第2の実施形態にかかるドキュメント保護プログラムの処理を示す図である。

【図24】 第2の実施形態にかかるドキュメント保護プログラムおよびアクセスコントロールサーバの動作の流れを示す図である。

【図25】 第2の実施形態にかかるドキュメント印刷プログラムおよびアクセスコントロールサーバの動作の流れを示す図である。

【図26】 プリンタが備えるセキュリティ機能の例を示す図である。

【図27】 PACが設定されたドキュメントを印刷する際の処理を示す図である。

【図 2 8】 P I N 入力ダイアログを示す図である。


【図 2 9】 ドキュメントを複数のセグメントに分けて保護する場合の処理を示す図である。

【図 3 0】 ドキュメント保護プログラムをリモートサーバ上に配置した状態を示す図である。

【符号の説明】

【 0 2 1 1 】

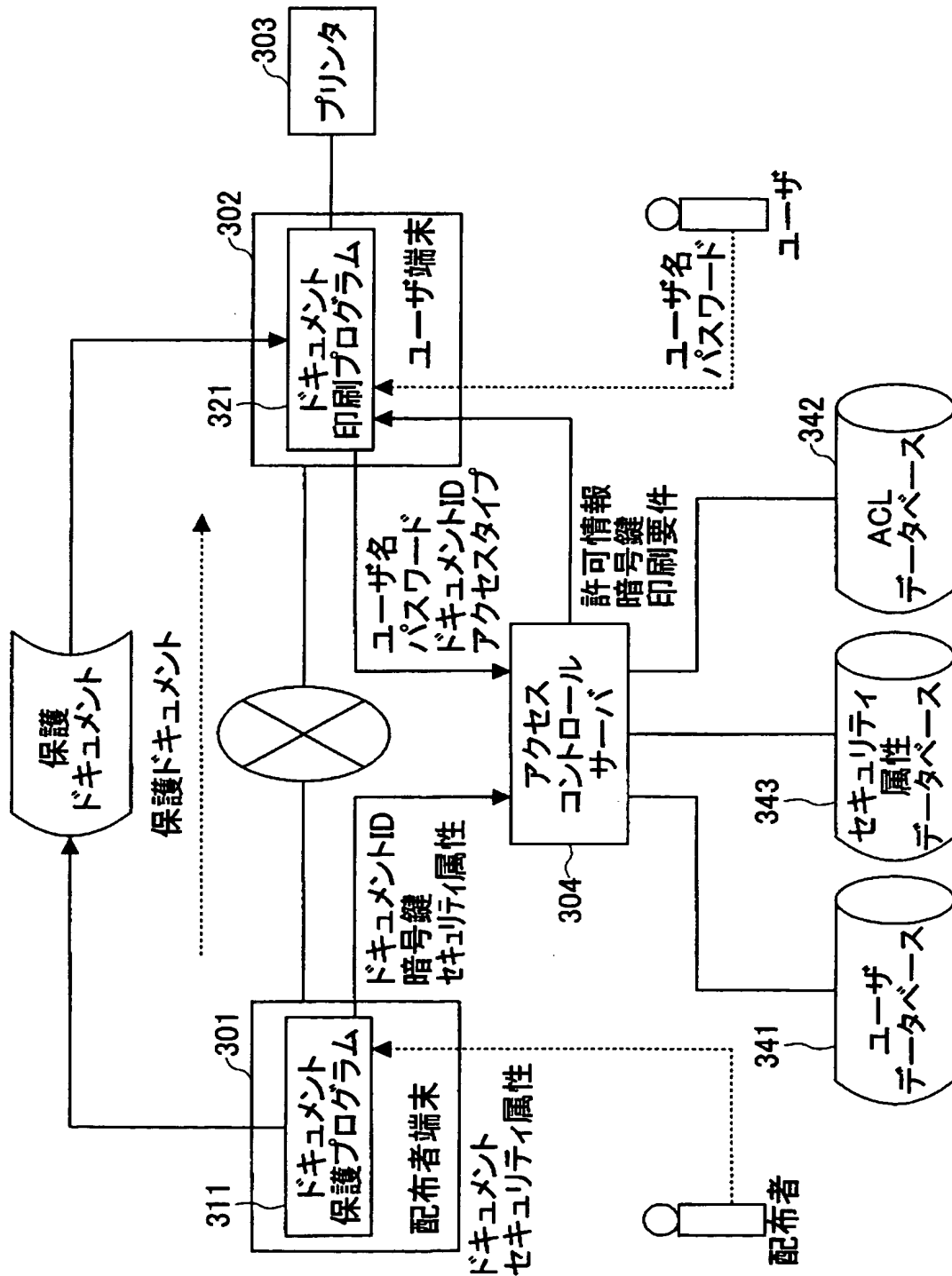
3 0 1	配布者端末
3 0 2	ユーザ端末
3 0 3	プリンタ
3 0 4	アクセスコントロールサーバ
3 4 1	ユーザデータベース
3 4 2	A C L データベース
3 4 3	セキュリティ属性データベース
3 1 1	ドキュメント保護プログラム
3 2 1	ドキュメント印刷プログラム
3 1 1 a	暗号化部
3 1 1 b	暗号鍵取得部
3 1 1 c	属性付与部
3 1 1 d	属性登録部
3 1 1 e	パラメータ取得部
3 2 1 a	復号部
3 2 1 b	復号鍵取得部
3 2 1 c	印刷要件取得部
3 2 1 d	印刷処理部
3 2 1 e	要件処理部
3 2 1 f	ドキュメント加工部
3 2 1 g	プリンタドライバ
3 2 1 h	警告表示部
3 2 1 i	ログ記録部
3 2 1 j	パラメータ取得部
3 0 4 a	属性 D B 登録部
3 0 4 b	ユーザ認証部
3 0 4 c	アクセス権限確認部
3 0 4 d	印刷要件取得送付部
4 0 1	配布者端末
4 0 2	ユーザ端末
4 0 3	プリンタ
4 0 4	アクセスコントロールサーバ
4 1 1	ドキュメント保護プログラム
4 2 1	ドキュメント印刷プログラム
4 4 1	ユーザデータベース
4 4 3	セキュリティ属性データベース
4 4 4	セキュリティポリシー
4 1 1 a	暗号化部
4 1 1 b	暗号鍵取得部
4 1 1 c	属性付与部
4 1 1 d	属性登録部
4 1 1 e	パラメータ取得部
4 2 1 a	復号部



4 2 1 b	復号鍵取得部
4 2 1 c	印刷要件取得部
4 2 1 d	印刷処理部
4 2 1 e	要件処理部
4 2 1 f	ドキュメント加工部
4 2 1 g	プリンタドライバ
4 2 1 h	警告表示部
4 2 1 i	ログ記録部
4 2 1 j	パラメータ取得部
4 0 4 a	属性 D B 登録部
4 0 4 b	ユーザ認証部
4 0 4 c	アクセス権限確認部
4 0 4 d	印刷要件取得送付部

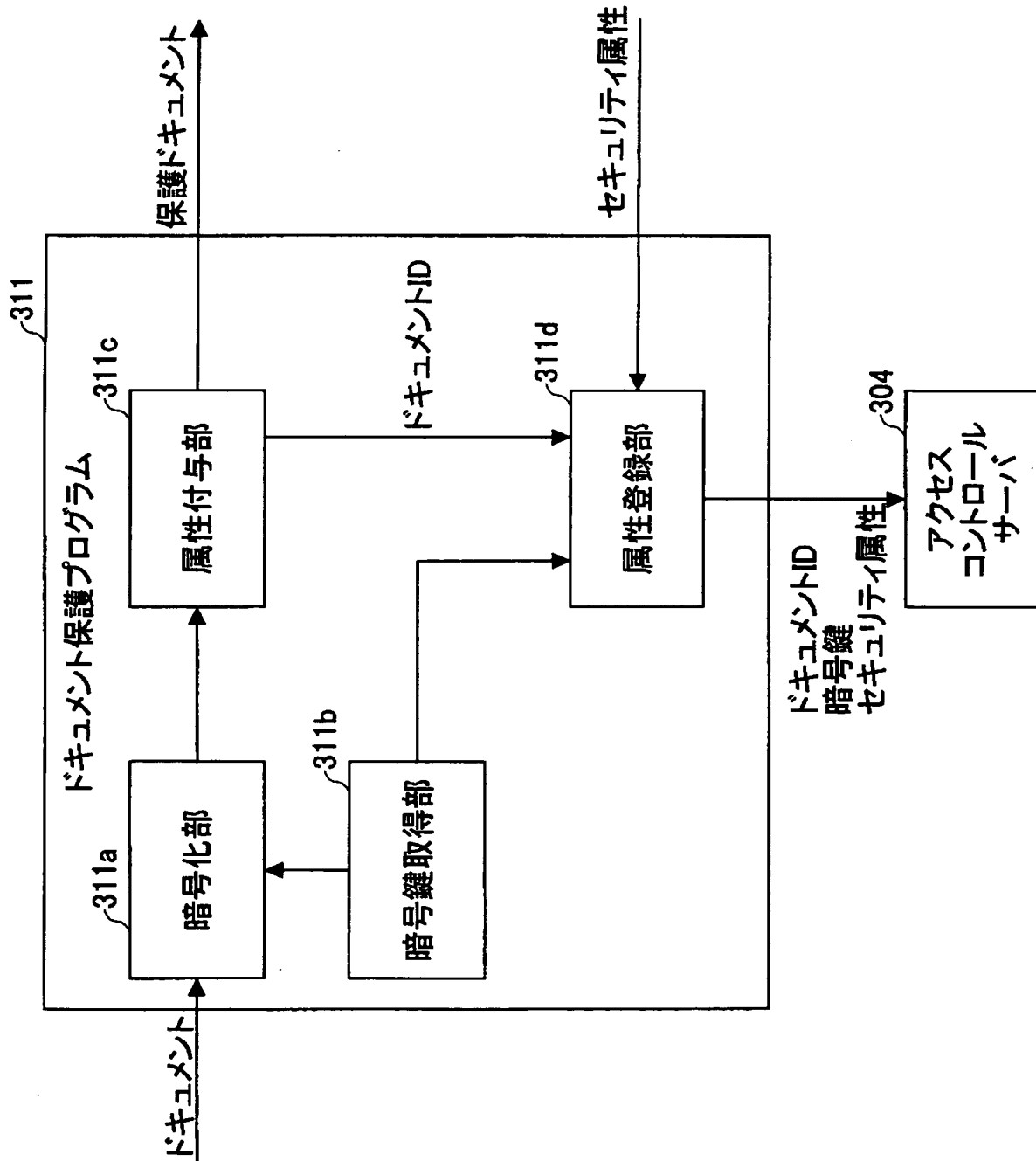
【書類名】 図面
【図 1】

本発明を好適に実施した第1の実施形態にかかる
ドキュメント保護・印刷システムの構成を示す図



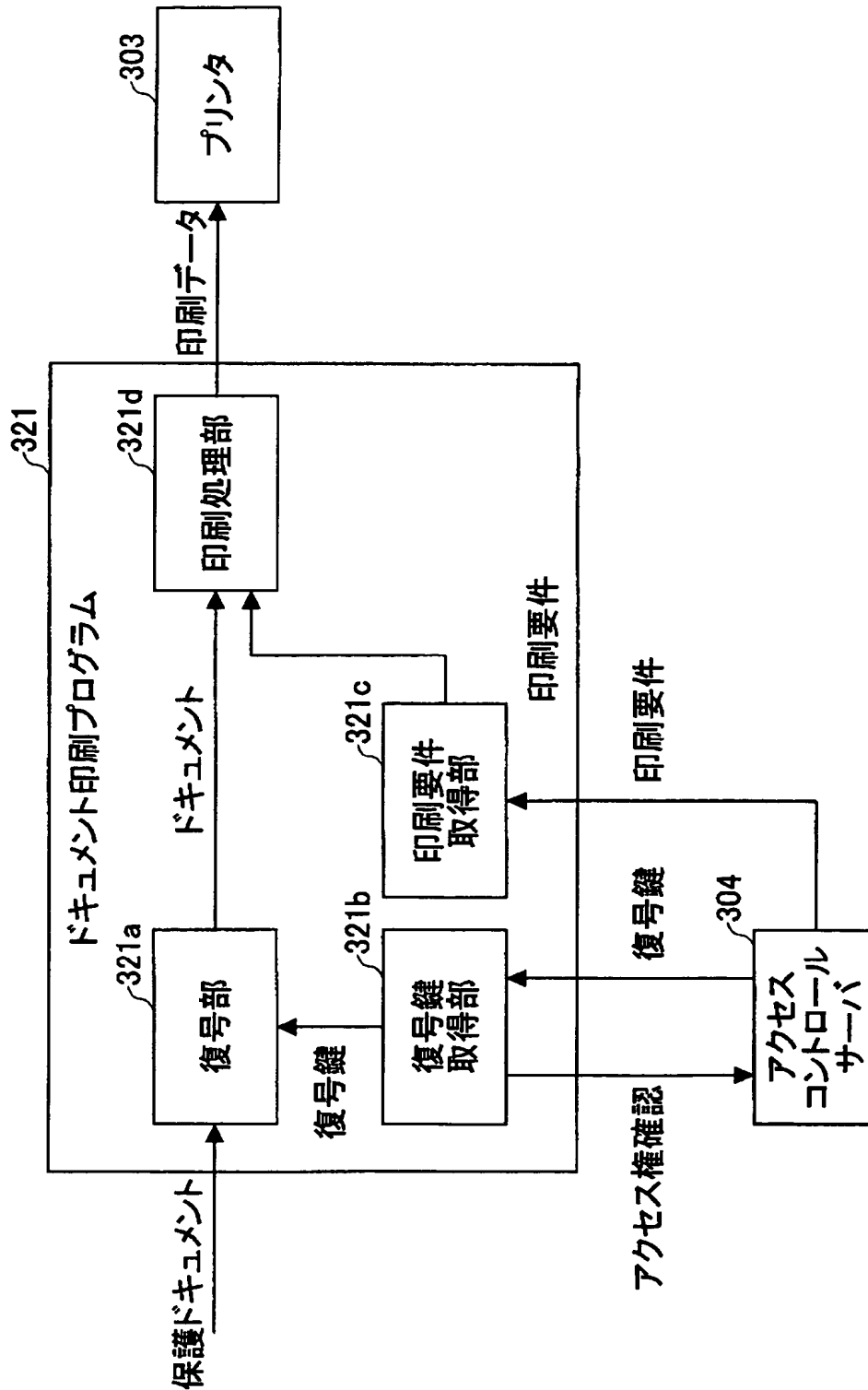
【図 2】

ドキュメント保護プログラムの構成例を示す図



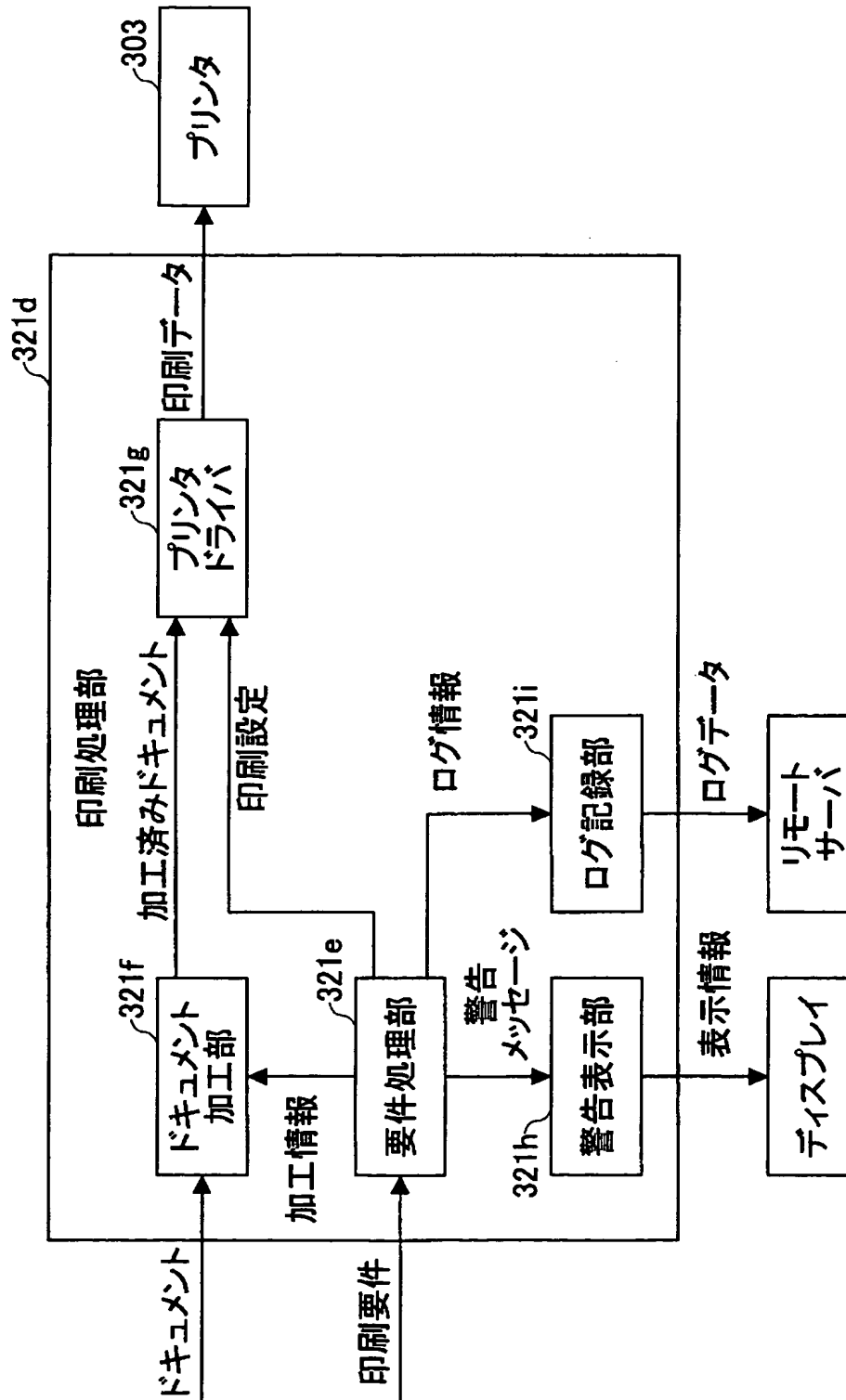
【図 3】

ドキュメント印刷プログラムの構成例を示す図



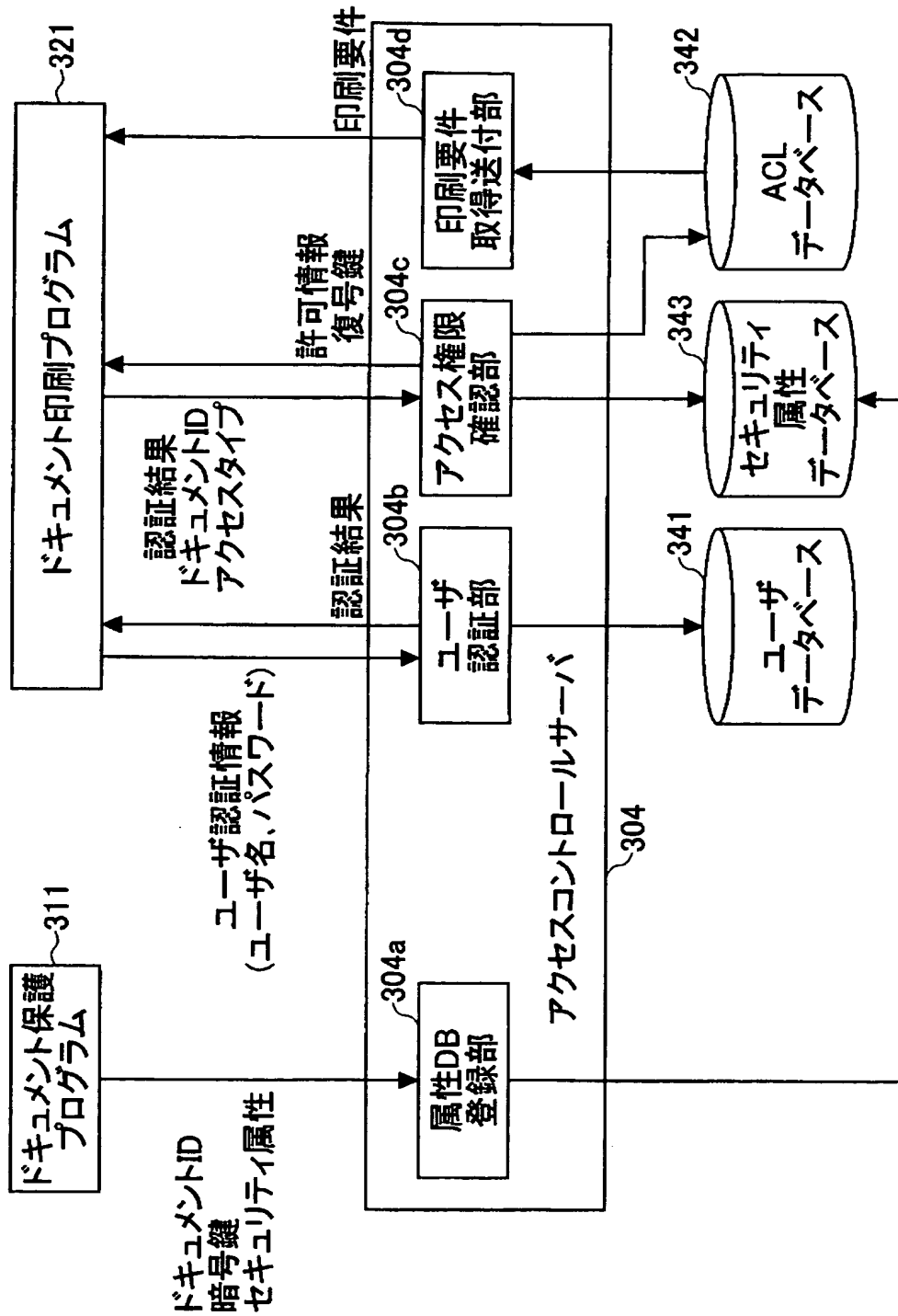
【図 4】

印刷処理部の構成例を示す図



【図 5】

アクセスコントロールサーバの構成例を示す図



【図 6】

ACLの構成例を示す図

User name	Access type	Permission	Requirement
Ichiro	Read	Allowed	—
	Write	Denied	—
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Patten)
			EBC(Embedding BarCode)
	Hardcopy	Allowed	RAD(Record Audit Date)
Taro	Read	Allowed	—
	Write	Denied	—
	Print	Denied	—
	Hardcopy	Denied	—
⋮			

【図 7】

セキュリティ属性の設定を要求する画面の例を示す図

文書のセキュリティ属性

文書カテゴリ

機密レベル

ファイル:

【図 8】

ユーザ名(ユーザID)とパスワードを要求する画面の例を示す図

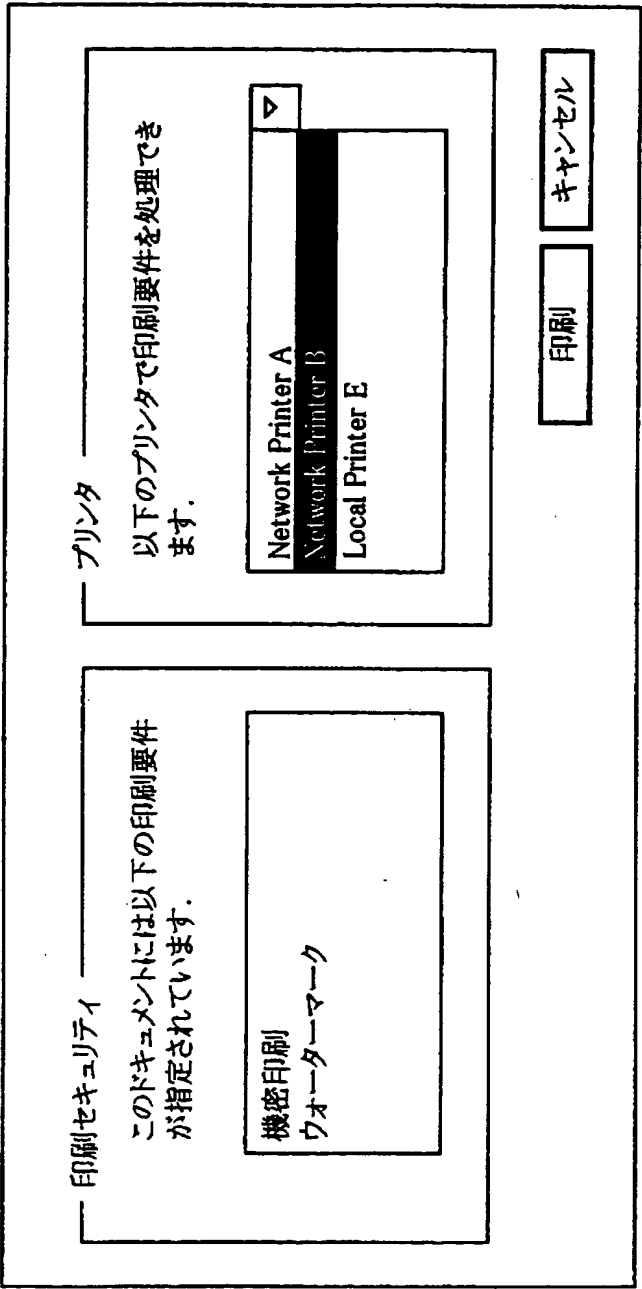
SecurePDF ユーザ認証

ユーザID

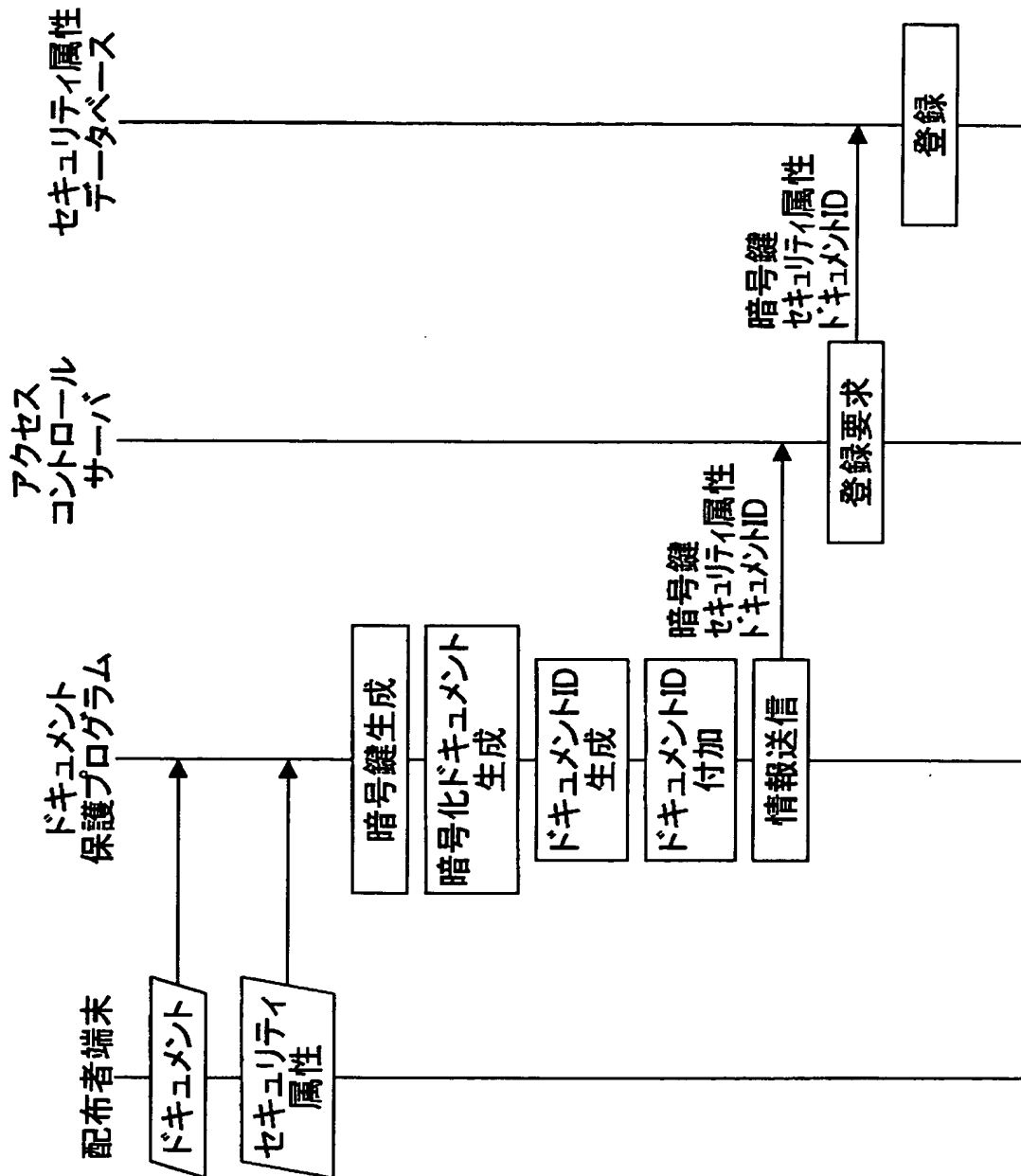
パスワード

【図 9】

ユーザ端末の表示装置上に表示される確認画面の例を示す図

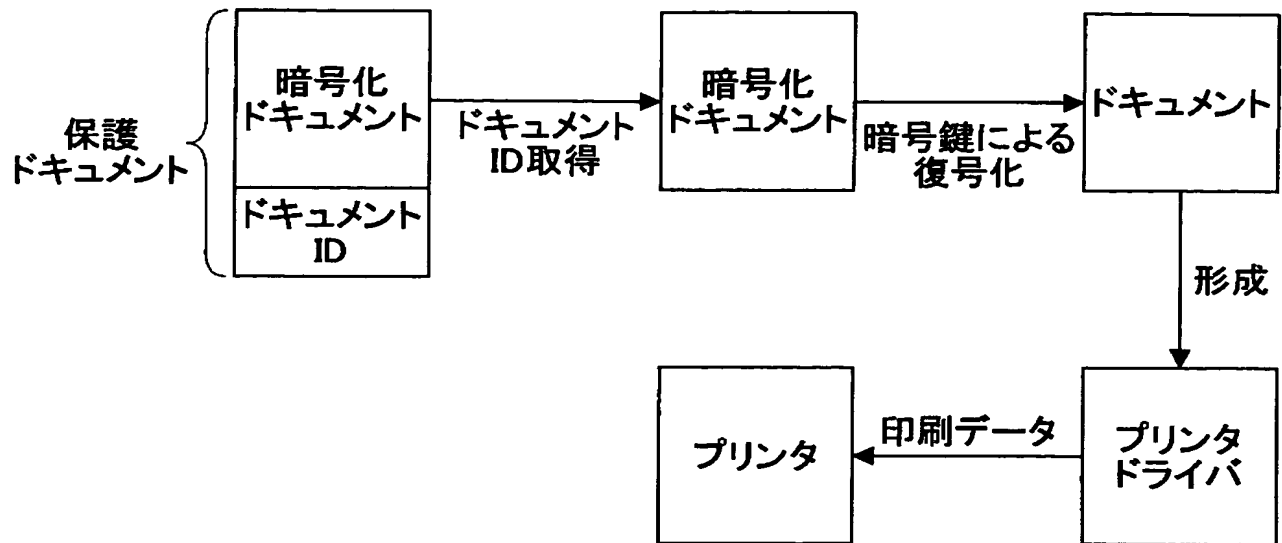


【図 10】

第1の実施形態にかかるドキュメント保護プログラムおよび
アクセスコントロールサーバの動作の流れを示す図

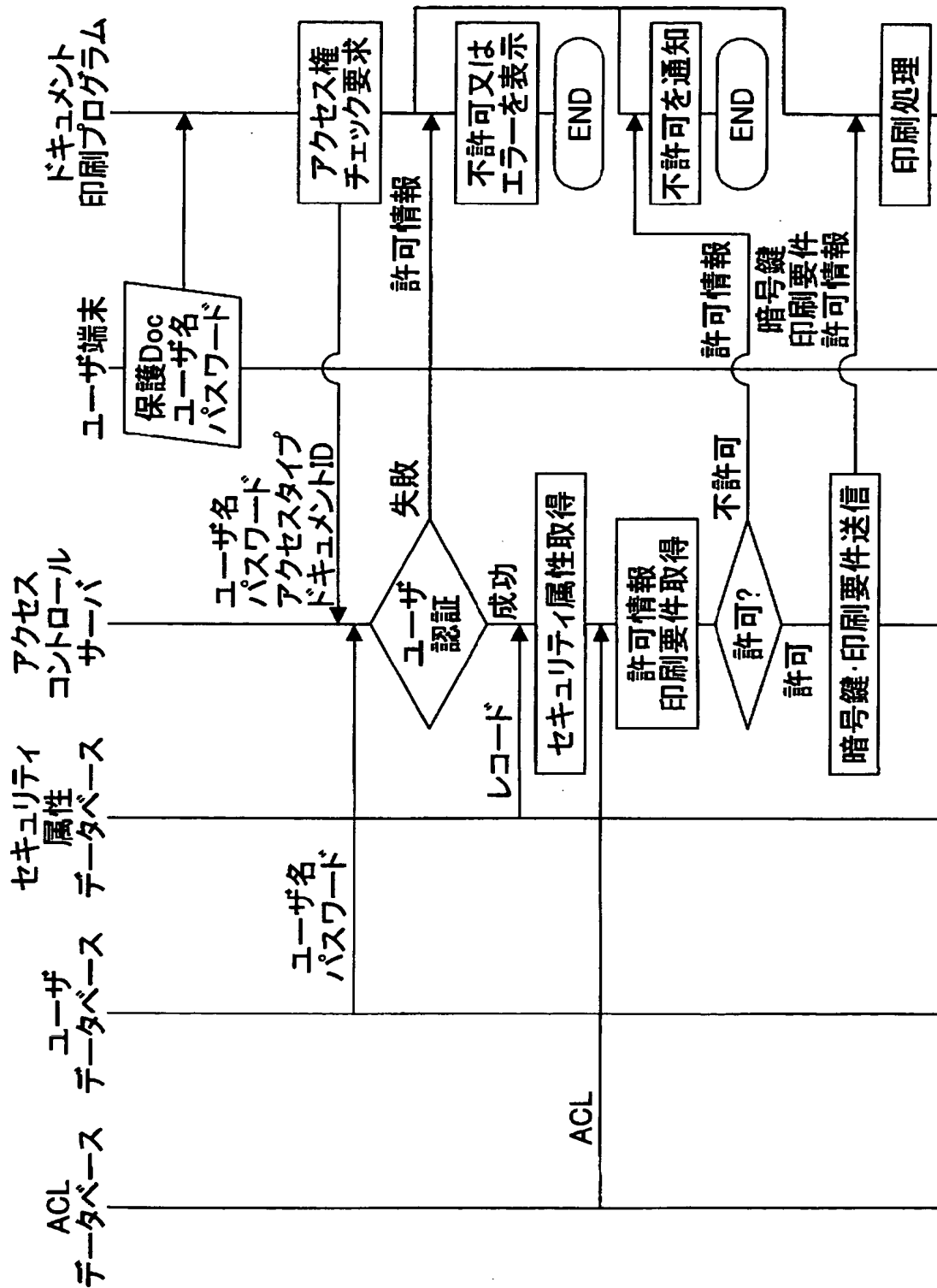
【図 11】

第1の実施形態にかかるドキュメント印刷プログラムの動作を示す図



【図 12】

第1の実施形態にかかるドキュメント印刷プログラムおよび
アクセスコントロールサーバの動作の流れを示す図



【図 13】

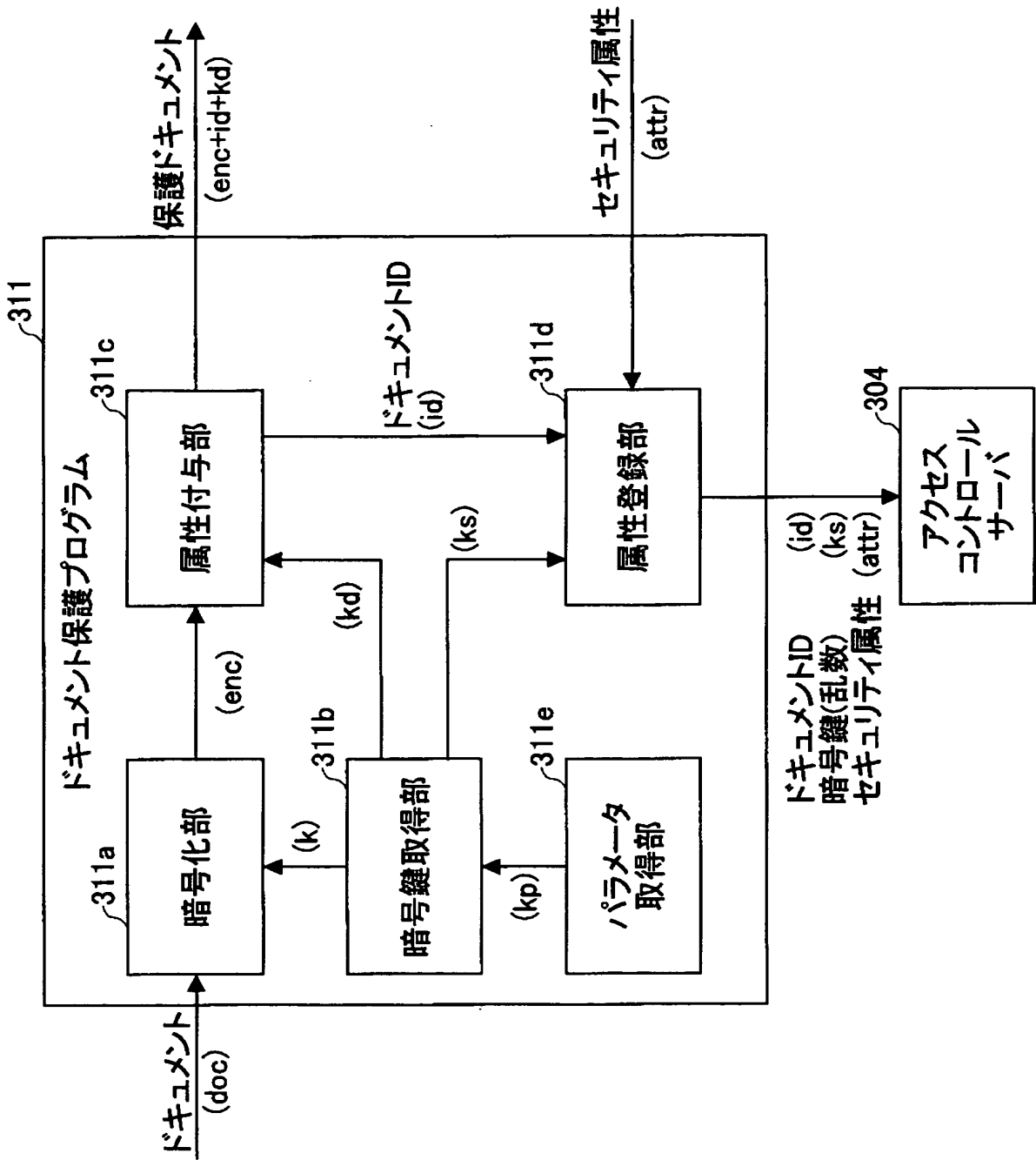
アクセスコントロールサーバへのSOAPによる 問い合わせの例を示す図

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <s:Body>
    <m:isAllowed xmlns:m="http://sample.com/sample">
      <sessionId>adfkla;iowoemads</sessionId>
      <userId>taro.yamada</userId>
      <docId>shm000000000003</docId>
      <accessType>print</accessType>
    </m:isAllowed>
  </s:Body>
</s:Envelope>
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <s:Body>
    <m:isAllowedResponse xmlns:ns1="http://sample.com/sample">
      <isAllowedReturn>
        <allowed xsi:type="xsd:boolean">true</allowed>
        <requirements>
          <item>
            <requirement>private_access</requirement>
          </item>
          <item>
            <requirement>watermark</requirement>
          </item>
          <supplement>CONFIDENTIAL</supplement>
        </requirements>
      </isAllowedReturn>
    </m:isAllowedResponse>
  </s:Body>
</s:Envelope>
```

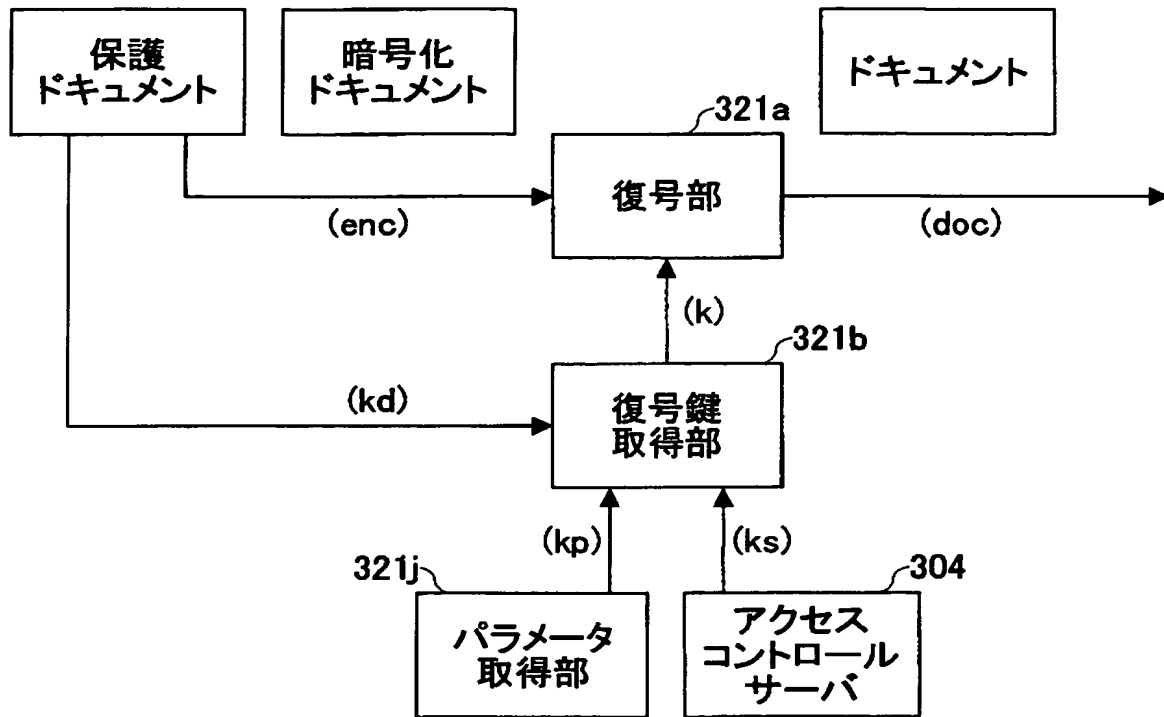
【図 14】

ドキュメント保護プログラムの構成例を示す図



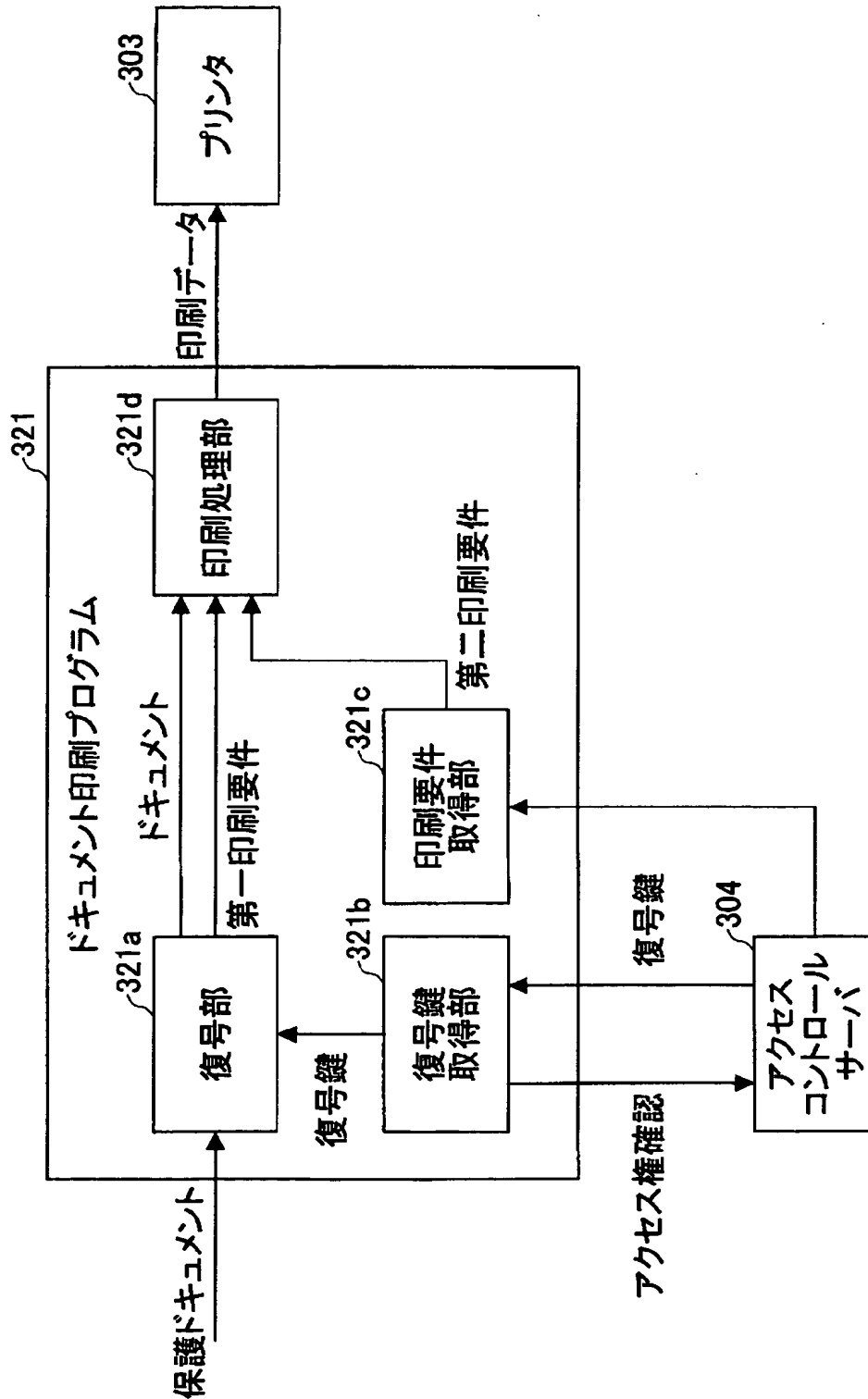
【図 15】

復号の様子を示す図



【図 16】

ドキュメント印刷プログラムの構成例を示す図



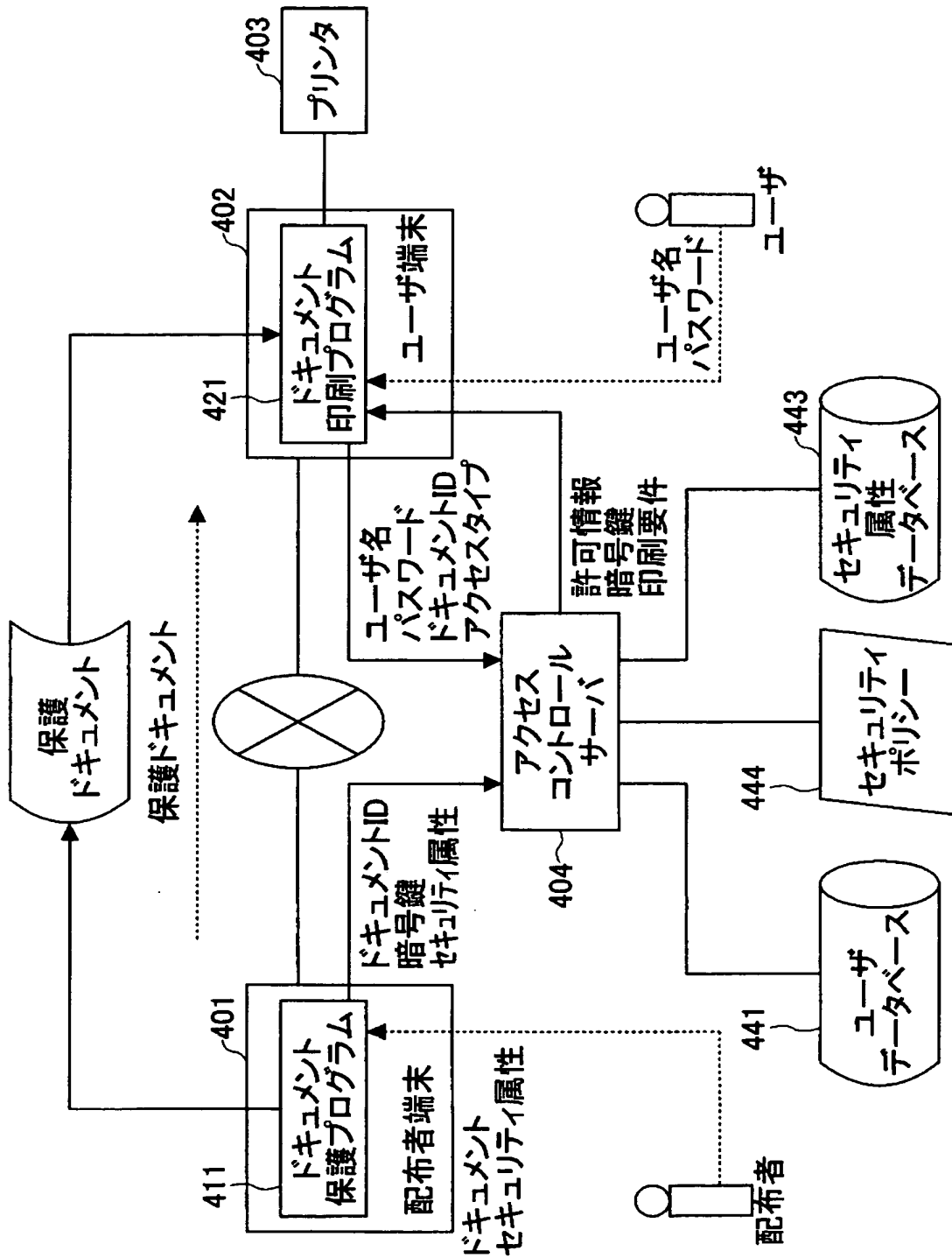
【図 17】

セキュリティポリシーの例を示す図

極秘文書について：	
原則複写禁止	複写する際には管理責任者の許可を得なければならない。また、複写したことを記録しておかなければならない。プリントする際には複写禁止であることを示す透かしを入れなければならない。また、プリントしたことを記録しておかなければならない。
閲覧は関係者のみ許可	
丸秘文書について：	
複写は関係者のみ許可	複写は関係者のみ許可
プリントする際には丸秘文書であることを示すラベルを同時に印刷しなければならない。	
閲覧は関係者のみ許可	
社外秘文書について	
社外へ送付する際には管理者の許可を得なければならない。	
複写・プリント・閲覧は社内であれば許可不要	
人事関連文書について	
全て丸秘文書として扱う	
・	
・	
・	
・	

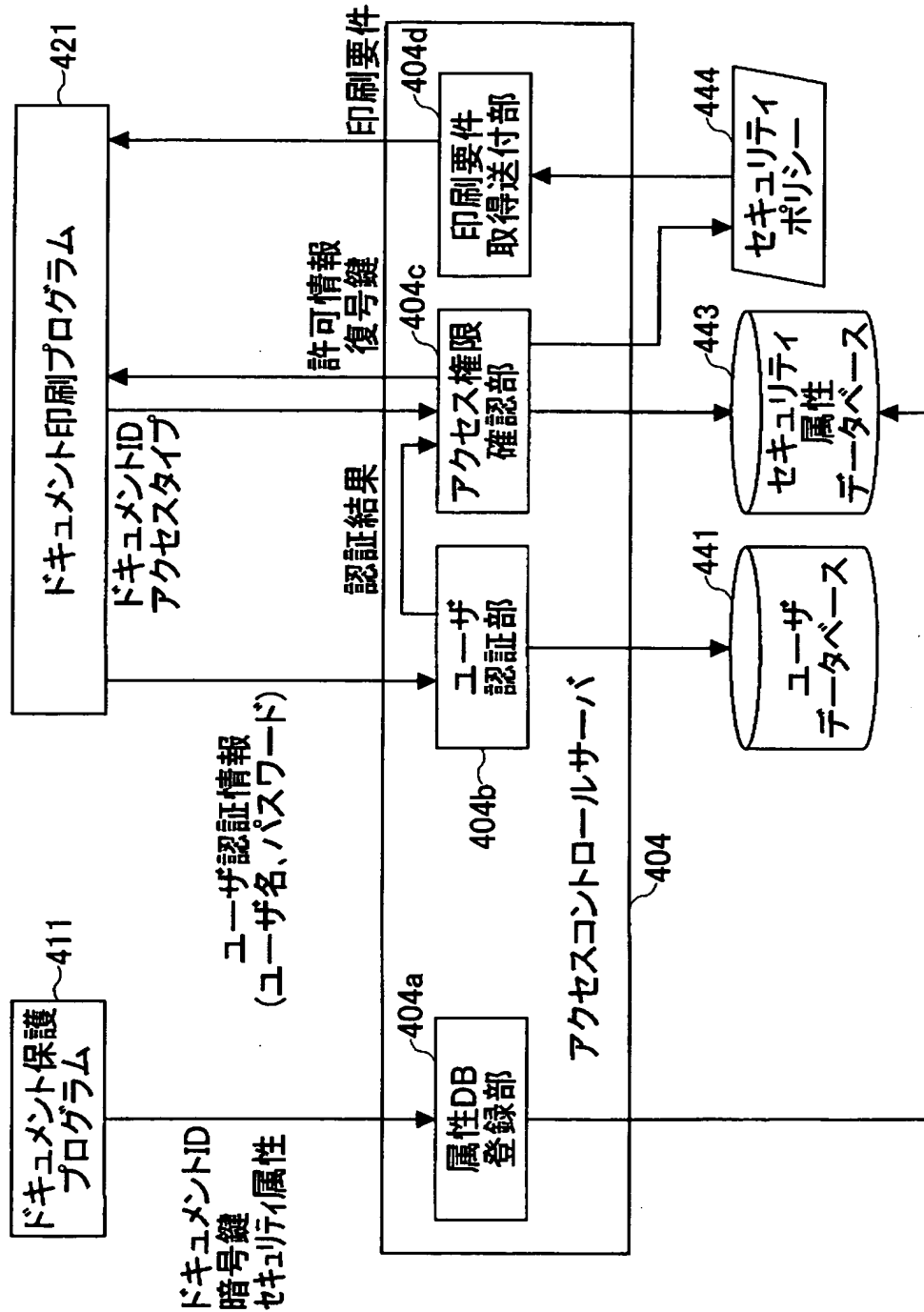
【図 18】

本発明を好適に実施した第2の実施形態にかかる
ドキュメント保護・印刷システムの構成を示す図



【図 19】

アクセスコントロールサーバの構成例を示す図



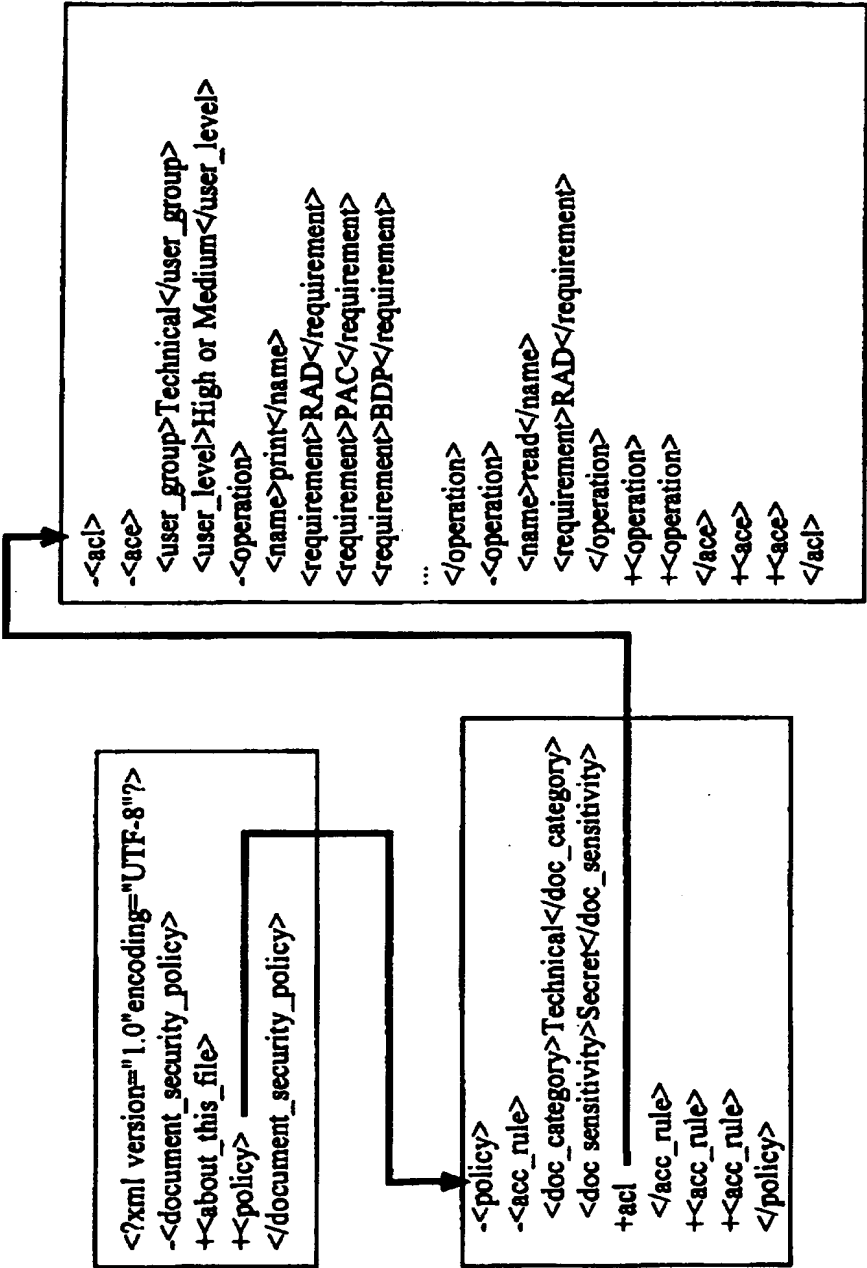
【図 2 0】

セキュリティポリシーを電子データとした場合のデータ構造を示す図

Document Type		User Type		Access Type	Permission	Requirement
Category	Sensitivity	Category	Level			
Technical	Secret	Technical	Medium High	Read	Allowed	RAD
				Print	Allowed	PAC BDP EBC RAD
				Hardcopy	Denied	
				...		
Technical	Top Secret	Technical	High	...		
Human Resource	Top Secret	Human Resource	High	...		
				Read	Allowed	RAD
				Print	Denied	
				Hardcopy	Denied	

【図 21】

セキュリティポリシーを電子データとして記述した例を示す図



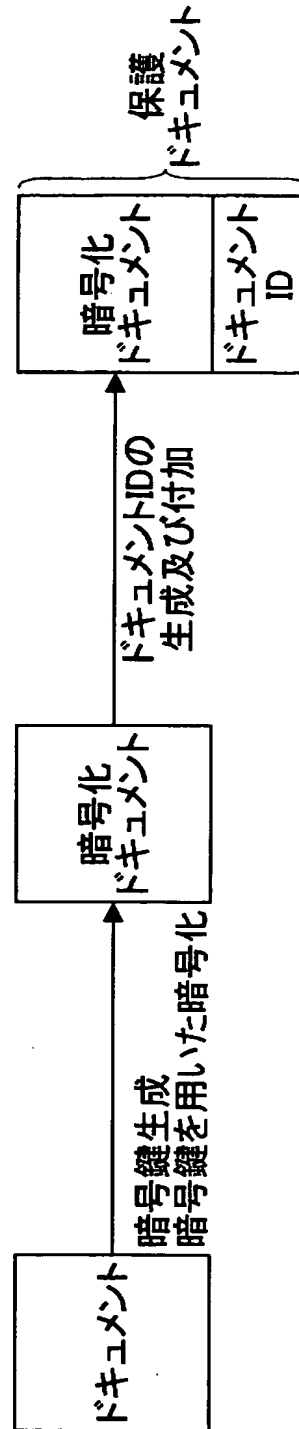
【図 2 2】

ユーザデータベースに記録される情報の構造例を示す図

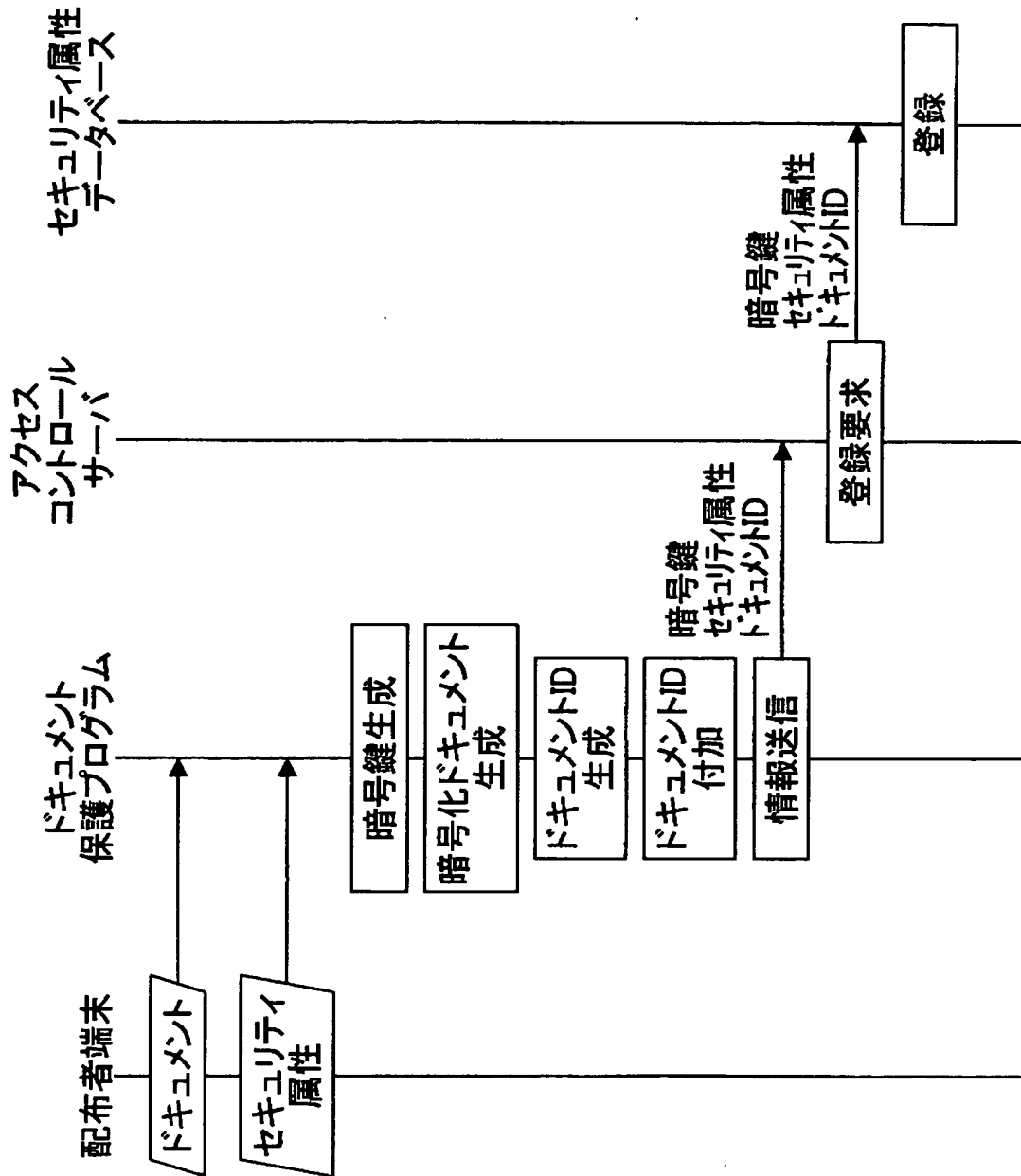
User name	Password	Category	Level
Ichiro	98q34rah	Technical	Medium
		General	Basic
Taro	Adoijoqer	Human Resource	Top Secret
		General	Basic
⋮			

【図 23】

第2の実施形態にかかるドキュメント保護プログラムの処理を示す図

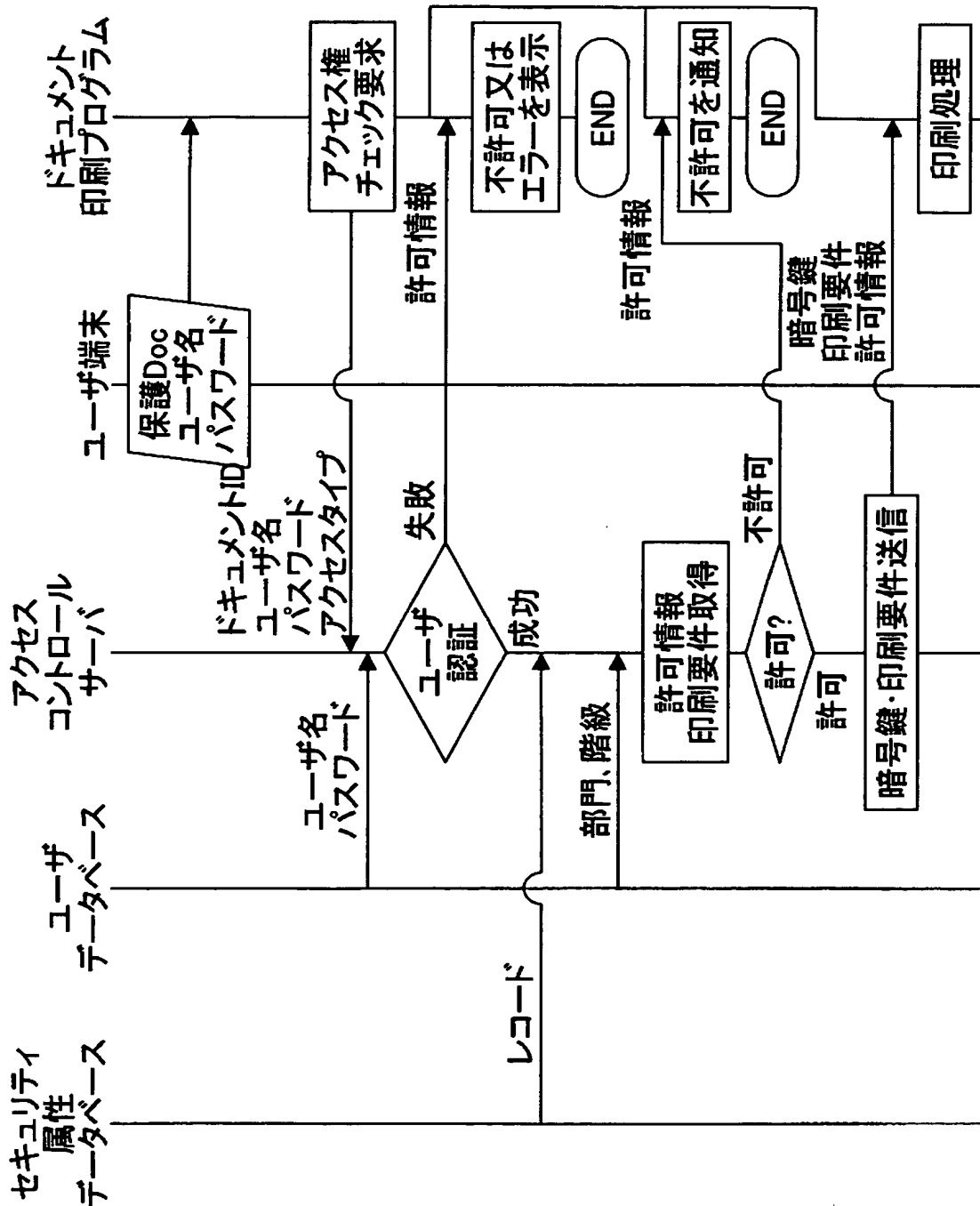


【図 24】

第2の実施形態にかかるドキュメント保護プログラムおよび
アクセスコントロールサーバの動作の流れを示す図

【図 25】

第2の実施形態にかかるドキュメント印刷プログラムおよび
アクセスコントロールサーバの動作の流れを示す図



【図 2 6】

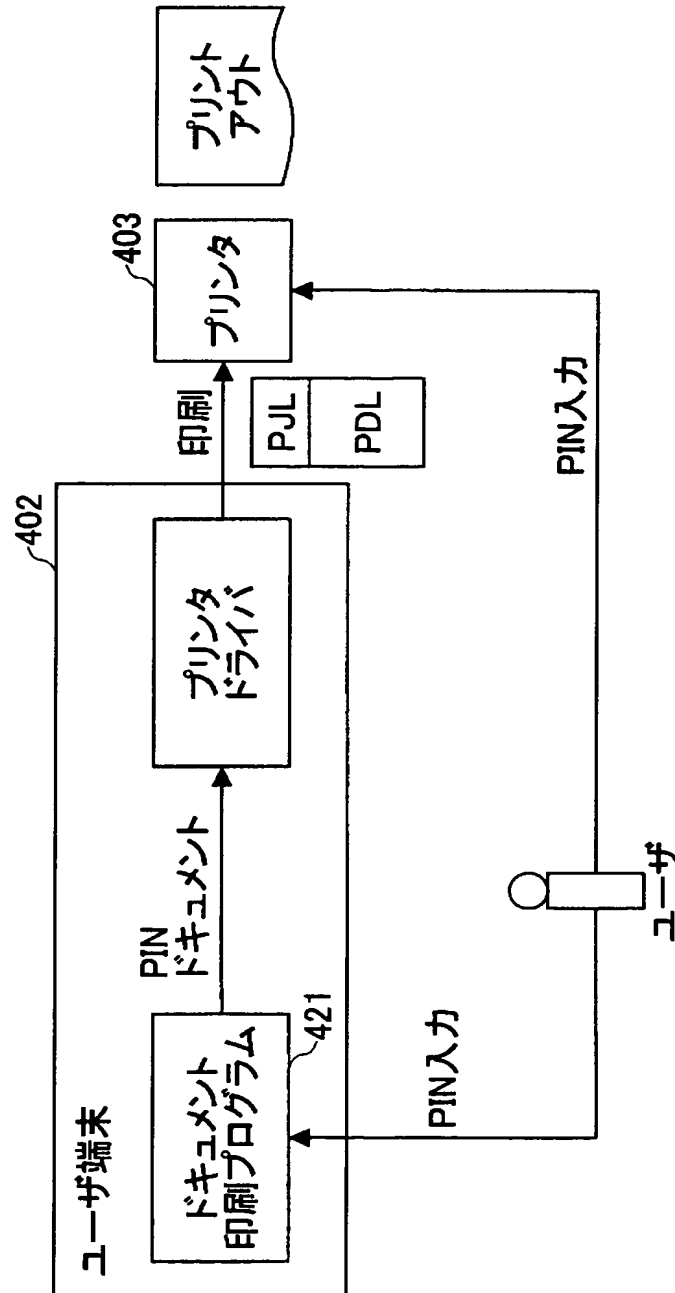
プリンタが備えるセキュリティ機能の例を示す図

プリントセキュリティ機能

スタンプ機能	マル秘などのマークをスタンプやウォーターマークとしてページ内の任意の場所に重ねて印刷する機能。スタンプに使用することができるのは「秘」や「CONFIDENTIAL」などの文字列やビットマップ画像である。
地紋印刷機能	複写機で複写されると特定のイメージが浮き上がるようにコントロールした地紋画像を原稿に重ね合わせて印刷する機能。上記のスタンプ機能でスタンプとして指定する画像を地紋画像にすることで実現する手法が一般的である。
機密印刷機能	印刷を指示する際にプリンタドライバに P I N (Personal Identification Number) を指定すると、印刷した本人がプリンタのところへ行き、プリンタのオペレーションパネルでその P I N を入力しなければプリントアウトされない機能。

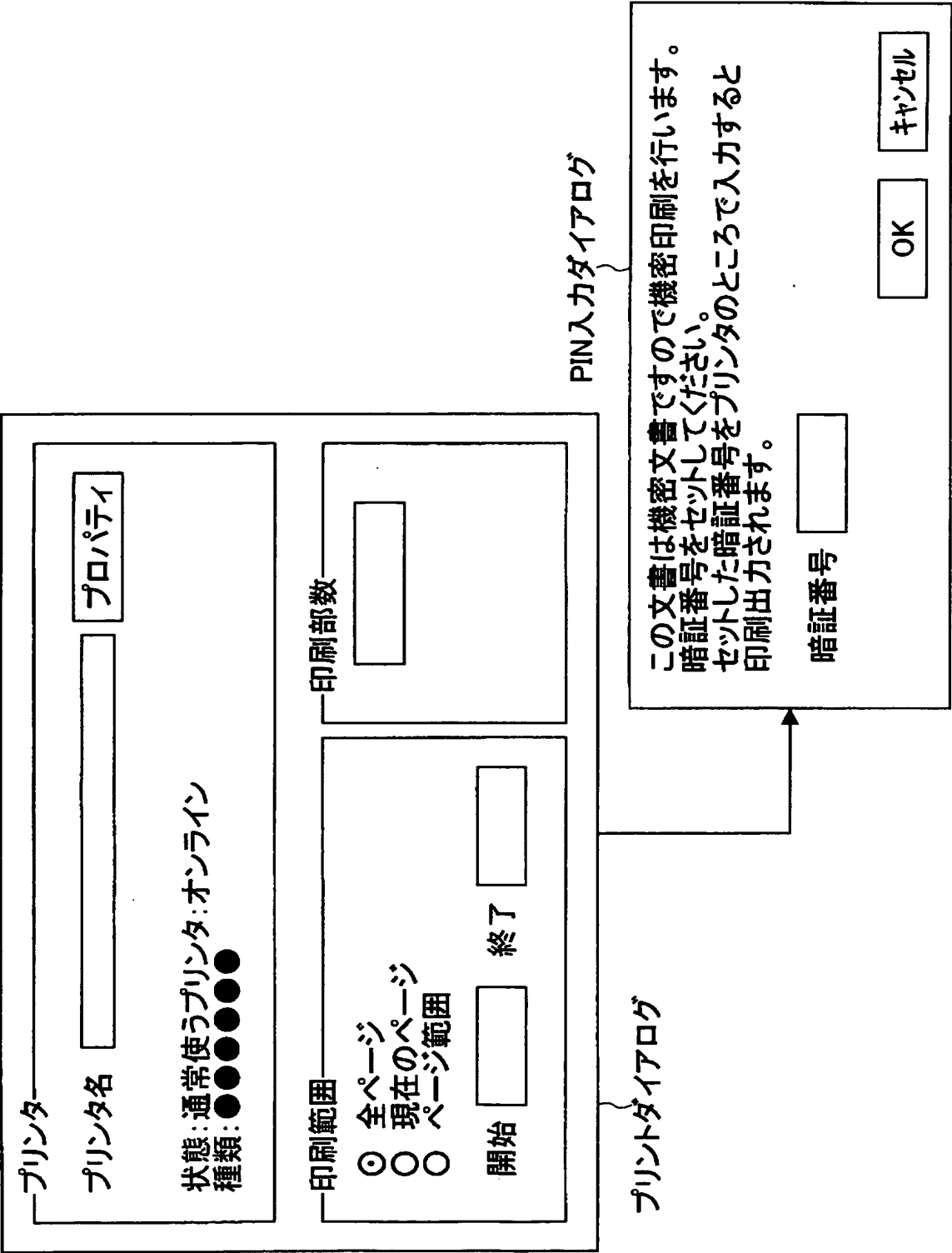
【図 27】

PACが設定されたドキュメントを印刷する際の処理を示す図



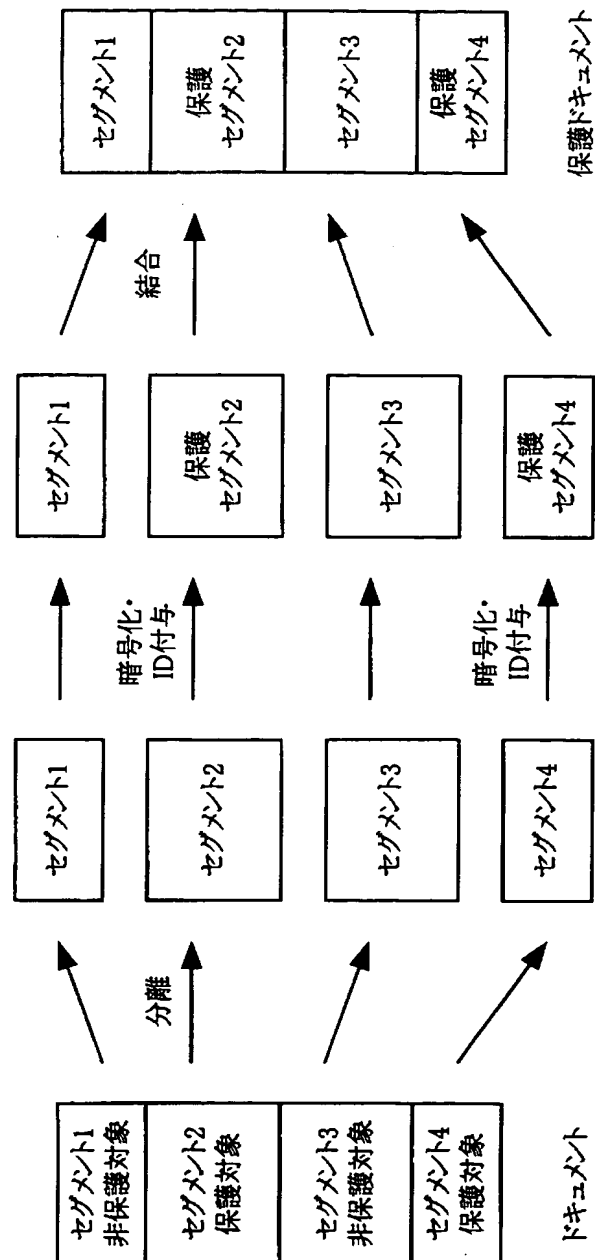
【図 28】

PIN入力のダイアログを示す図



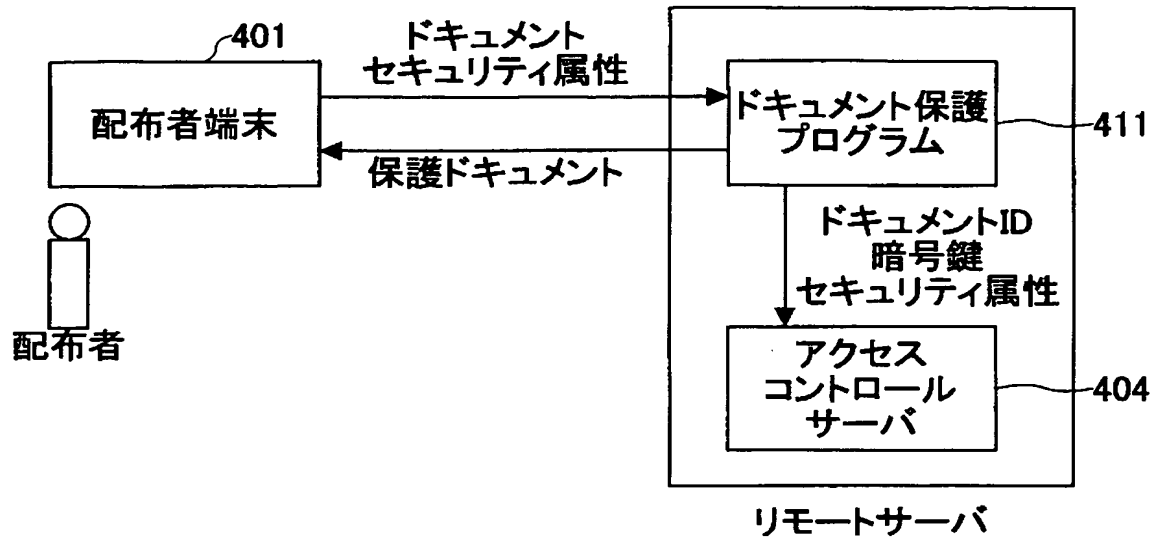
【図 29】

ドキュメントを複数のセグメントに分けて保護する場合の
処理を示す図



【図 30】

ドキュメント保護プログラムをリモートサーバ上に
配置した状態を示す図



【書類名】 要約書**【要約】**

【課題】 プリントアウトによるドキュメントの漏洩を防止したドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムを提供することを目的とする。

【解決手段】 暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件をネットワークを介してサーバから取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とを備えるドキュメント印刷プログラムと、ドキュメントファイルの保護を行うドキュメント保護プログラムとにより構成される。

【選択図】 図 1

特願 2 0 0 3 - 3 1 4 4 6 6

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー